AUDIT DES AUTORISATIONS NUMÉRIQUES

Bureau de la vérification et de l'évaluation

National Research Council Canada
Conseil national de recherches Canada
Canada

NRC.CANADA.CA

Exemple 1 : Utilisé lorsqu'un seul format de publication est créé.

Nº de catalogue: NR16-380/2022F-PDF

ISBN: 978-0-660-42788-1

Also available in English

NRC.CANADA.CA

TABLE DES MATIÈRES

Sommaire et conclusion

Contexte

En raison de la pandémie de la COVID-19 qui oblige les employés à travailler à distance, le Conseil national de recherches du Canada (CNRC) a dû s'adapter pour assurer la continuité de ses activités. Il existe un contraste frappant entre un environnement de travail au bureau et un environnement à distance. Un environnement de travail à distance nécessite une adaptation tant de la part de l'employé que de l'organisation. L'un des ajustements nécessaires est le passage de l'utilisation de signatures « manuscrites » à d'autres méthodes d'autorisation numérique. En avril 2020, une directive sur l'autorisation numérique a été publiée pour orienter la mise en œuvre des méthodes d'autorisation numérique dans les processus commerciaux. Compte tenu de la rapidité avec laquelle cette transformation a été réalisée et de la période où elle a été effectuée, la présente vérification visait à s'assurer qu'une surveillance appropriée avait été appliquée.

En juillet 2019, le Conseil du Trésor (CT) a publié le document intitulé *Orientation du gouvernement du Canada sur l'utilisation des signatures électroniques*. Ce document s'adresse aux ministères et organismes du gouvernement du Canada qui envisagent d'utiliser l'autorisation numérique à l'appui de leurs activités quotidiennes. Il existe quatre types d'autorisations numériques : (1) la signature numérique, (2) la signature électronique, (3) l'approbation du système, et (4) l'approbation par courriel. Chacune de ces autorisations s'appuie sur des outils différents qui fournissent un niveau d'assurance différent pour minimiser le risque.

Les termes « signature électronique » et « signature numérique » sont souvent utilisés de manière interchangeable, mais n'ont pas le même sens. Une signature électronique saisit les informations relatives à la personne qui a signé, au document signé, au moment de la signature et à la manière dont cette signature a été incorporée, jointe ou associée à un document électronique. Elle convient aux transactions à risque faible ou modéré, car il n'est pas nécessaire dans de tels cas de contrôler le contenu ni de valider l'identité du signataire. Une signature numérique découle d'une transformation de données qui s'opère par l'entremise d'un système de clés cryptographiques. Associée à un certificat de signature, tel que Entrust (maCLÉ), celle-ci permet à la personne qui reçoit le document signé de déterminer si la signature a été créée à l'aide de la clé cryptographique qui correspond à celle du signataire et si elle a été modifiée depuis.

Les transactions basées sur l'approbation d'un système réalisées par l'entremise d'une approbation du flux de travail intégré ne nécessitent pas de certificat de signature, car celles-ci sont effectuées dans un système à l'aide d'identifiants de système sécurisés, par exemple le système de voyage SAP, les approbations de factures SAP, etc. Les approbations par courriel peuvent être utilisées pour approuver des opérations internes à faible risque.

Les risques inhérents à l'utilisation des signatures numériques dans toute organisation sont l'authentification, la recevabilité et la conformité. Les signatures numériques, qui obligent l'employé à saisir des informations d'identification avant de signer et sont souvent horodatées, ce qui renforce l'authenticité d'une signature. Les signatures numériques peuvent également « verrouiller » le document, en interdisant toute modification du document signé.

Dans le cadre du processus de planification annuelle basée sur les risques pour 2021-2022, le Bureau de la vérification et de l'évaluation du CNRC a déterminé que la vérification des

contrôles clés était une priorité élevée. L'autorisation numérique était l'une des composantes relevées comme présentant un risque élevé dans le cadre des contrôles clés.

Opinion et conclusion de la vérification

En tant que dirigeante principale de la vérification, j'estime dans l'ensemble que la conception de la transition vers l'autorisation numérique était bien établie et conforme aux directives du CT. Toutefois, l'opérationnalisation des signatures numériques pourrait être améliorée, notamment en ce qui concerne le contrôle de la conformité.

Principaux points à retenir

Dans l'ensemble, la vérification a permis de constater que le CNRC a élaboré, approuvé, communiqué et mis à jour la directive sur l'autorisation numérique avant sa mise en œuvre, conformément au document *Orientation du gouvernement du Canada sur l'utilisation des signatures électroniques.* La directive intérimaire du CNRC sur l'autorisation numérique a été approuvée en avril 2020. On a mené un examen de la directive, des pratiques et des risques et la directive révisée a été présentée au Comité de gestion de la sécurité (CGS) le 22 septembre 2021 à des fins d'approbation. La directive établit le format numérique comme la méthode privilégiée pour autoriser et approuver les transactions opérationnelles et fournit le cadre permettant aux responsables de processus opérationnels de choisir le mécanisme d'approbation approprié en fonction du niveau d'assurance requis pour la transaction ou l'activité opérationnelle.

La directive documente la gouvernance, les rôles et les responsabilités et les attribue à tous les intervenants pertinents du CNRC. Bien que ces informations soient correctement documentées, il se peut que certaines responsabilités n'aient pas été clairement communiquées. Lors de discussions avec les principaux intervenants, il a été constaté que tous les responsables de processus opérationnels n'étaient pas au fait de la responsabilité d'établir, de documenter et de communiquer les outils numériques acceptés pour chaque type de transaction ou processus opérationnel.

On a mené une évaluation des activités et des transactions opérationnelles avant de passer à l'autorisation numérique afin de déterminer lesquelles d'entre elles devraient être approuvées pour l'utilisation de l'autorisation numérique, ainsi que la méthode d'autorisation numérique à utiliser. Les responsables des processus opérationnels ont pris part aux discussions d'un groupe de travail afin d'établir les niveaux d'assurance requis pour leurs activités et transactions opérationnelles respectives.

La vérification a révélé que les données et les enregistrements critiques des signatures numériques étaient sauvegardés. Cependant, d'après les entretiens réalisés, les pratiques de tenue des dossiers n'étaient pas toujours suivies conformément à la directive sur la gestion de l'information du CNRC (notamment les dispositions relatives au dépôt officiel). Les documents numériques doivent être conservés dans un dépôt numérique approuvé par le CNRC pour assurer la protection des données et garantir la non-répudiation de l'approbation numérique.

Avant d'adopter les autorisations numériques, des séances d'information ont été organisées, dont certaines étaient adaptées à des groupes particuliers. Des événements en direct incluant une période de questions ont également été organisés pour transmettre aux

employés des connaissances sur l'autorisation numérique. Ces séances étaient ouvertes à tous les employés du CNRC et les participants avaient la possibilité de poser des questions.

Bien que les employés aient été sensibilisés aux utilisations et aux limites de l'autorisation numérique par l'entremise de formations, d'instructions fournies sur MaZone[1] dans les guides « Comment faire » et de la directive intérimaire, des possibilités d'amélioration ont été relevées. Ces améliorations concernent spécifiquement la diligence raisonnable dans la validation d'une signature numérique pour les activités et les transactions opérationnelles qui présentent un risque.

Sur la base des entretiens tenus avec les responsables des processus opérationnelles, la vérification a permis d'établir les avantages considérables de la mise en œuvre des autorisations numériques par rapport aux signatures manuscrites. L'un de ces avantages est le renforcement des contrôles internes et de l'authentification des données. De plus, le gouvernement fédéral a commencé à favoriser l'utilisation de la technologie. Celle-ci a été largement acceptée par les banques, les autres institutions financières, le gouvernement et les grandes entreprises, ce qui accroît l'importance de son utilisation au sein du CNRC. La mise en œuvre de cette technologie, en plus des mécanismes de surveillance et des examens appropriés, contribuera à soutenir les efforts en cours pour numériser les opérations opérationnelles.

Recommandation

1. La vice-présidente des Services corporatifs et chef de la direction financière devrait mettre en œuvre un régime de surveillance axé sur les risques afin de contrôler la conformité aux exigences de la directive pour les processus opérationnels respectifs, y compris la validation des signatures numériques et l'assurance de la conservation des documents numériques dans un dépôt numérique approuvé du CNRC.

   [Priorité : **modérée**]

Énoncé de conformité

La présente mission de vérification a été réalisée conformément aux Normes internationales pour la pratique professionnelle de la vérification interne et au Code de déontologie de l'Institute of Internal Auditors (IIA), comme l'attestent les résultats du Programme d'assurance et d'amélioration de la qualité du CNRC.

Alexandra Dagger, vérificatrice interne certifiée, évaluatrice accréditée, dirigeante principale de la vérification

Remerciements

L'équipe de la vérification souhaite remercier ceux et celles qui ont collaboré à cet effort pour mettre en lumière les forces et les possibilités d'amélioration du CNRC liées à ce projet de vérification.

[1] MaZone : Site intranet pour les employés du CNRC.

1.0 Introduction

La majorité des employés du Conseil national de recherches Canada (CNRC) étant passés au télétravail en raison de la pandémie de la COVID-19, plusieurs processus opérationnels ont dû intégrer des méthodes de substitution d'approbation des documents. Les signatures manuscrites ont été remplacées par des méthodes d'autorisation numérique qui peuvent être approuvées depuis n'importe quel endroit. La mise en œuvre de ces méthodes était nécessaire pour assurer la continuité des activités de l'effectif travaillant à distance.

Pour orienter la transition vers l'utilisation de méthodes d'autorisation numérique, on a approuvé la nouvelle directive intérimaire du CNRC sur l'autorisation numérique en avril 2020. La directive :

- Établit que le format numérique est la méthode privilégiée pour autoriser et approuver les transactions opérationnelles effectuées par le CNRC;
- Fournit le cadre permettant aux responsables des processus opérationnels de choisir le mécanisme d'approbation approprié en fonction du niveau d'assurance requis pour le type de transaction opérationnelle.

Il existe quatre types d'autorisations numériques : (1) la signature numérique, (2) la signature électronique, (3) l'approbation du système, et (4) l'approbation par courriel. La vérification portait spécifiquement sur les signatures numériques. Au CNRC, une signature peut être considérée comme « numérique » lorsqu'elle est liée à un système cryptographique utilisant des clés, comme Entrust. Les signatures numériques offrent un niveau de sécurité plus élevé en exigeant une authentification par l'entremise d'un certificat Entrust émis par une source de confiance.

Pourquoi cette vérification est-elle importante?

Les mesures de distanciation sociale visant à ralentir la propagation de la COVID-19 ont nécessité la mise en œuvre immédiate de solutions gouvernementales virtuelles pour permettre au gouvernement de continuer à fournir des services aux Canadiens. Les employés travaillant à distance n'avaient plus accès aux imprimantes du bureau, ce qui compliquait l'autorisation de transactions internes qui nécessiteraient normalement des copies papier et des signatures manuscrites.

Bien que l'on utilisait depuis un certain temps les méthodes d'autorisation numérique (y compris l'approbation par courriel, les signatures électroniques, les signatures numériques et l'approbation du système) au sein du CNRC, avril 2020 a marqué la transition des signatures manuscrites vers l'autorisation numérique comme méthode privilégiée pour autoriser et approuver les activités et les transactions opérationnelles. Avec la transition du CNRC vers un environnement de travail à distance, la facilitation de l'autorisation numérique est devenue une nécessité.

Compte tenu de la rapidité avec laquelle cette transformation a été réalisée et de la période où elle a été effectuée, il est nécessaire d'assurer une clarté générale au sein de l'organisation au chapitre des exigences décrites dans la directive sur l'autorisation numérique.

2.0 À propos de la vérification

On a intégré la vérification au Plan d'audit axé sur les risques de 2022-2024 du CNRC, approuvé par le président le 30 juin 2021. La présente vérification a été réalisée par le Bureau de la vérification et de l'évaluation.

Objectif

L'objectif de la présente vérification était de s'assurer que les contrôles clés de la transition vers l'utilisation de l'autorisation numérique, par opposition aux signatures manuscrites, comme méthode privilégiée pour autoriser et approuver les activités et les transactions opérationnelles, étaient établis et appliqués comme prévu.

Portée

Cette vérification se concentrait sur les mesures prises avant avril 2020 en vue de la mise en œuvre et de l'utilisation par le CNRC de l'autorisation numérique comme méthode privilégiée pour autoriser et approuver les activités et les transactions opérationnelles.

Afin de déterminer la méthode d'autorisation numérique appropriée à utiliser, une évaluation a été réalisée en considérant les répercussions des menaces suivantes : usurpation d'identité, répudiation, perte d'intégrité des données et abus de pouvoir. Il existe quatre niveaux d'assurance qui requièrent une confiance faible, certaine, élevée ou très élevée dans le fait que la personne qui signe est bien celle qu'elle prétend être (tableau 1).

Tableau 1 : Niveaux d'assurance de l'identité (Ligne directrice sur l'assurance de l'identité)[2]

Niveau	Description
4	**Besoin d'un niveau très élevé d'assurance qu'une personne est celle qu'elle prétend être.** Une compromission pourrait raisonnablement entraîner des préjudices graves, sinon catastrophiques.
3	**Besoin d'un niveau élevé d'assurance qu'une personne est celle qu'elle prétend être.** Une compromission pourrait raisonnablement entraîner des préjudices modérés, sinon graves.
2	**Besoin d'une certaine assurance qu'une personne est celle qu'elle prétend être.** Une compromission pourrait raisonnablement entraîner des préjudices minimes, sinon modérés.
1	**Besoin d'un faible niveau d'assurance que la personne est celle qu'elle prétend être.** Une compromission pourrait raisonnablement entraîner des préjudices inexistants, voire minimes.

La vérification s'est concentrée sur les processus opérationnels nécessitant une assurance de niveau 2, étant donné que la plupart des opérations quotidiennes menées au sein du CNRC ne dépasseront pas ce niveau, comme l'explique la directive sur l'autorisation numérique du CNRC. Ces processus opérationnels comprennent le règlement de transactions par carte d'achat, les lettres d'offre et les accords de sous-traitance. Plus de 50 pour cent des activités et transactions opérationnelles nécessitant un niveau d'assurance 2 pour les signatures numériques relèvent de la Direction des services financiers et d'approvisionnement (figure 1).

[2] Ligne directrice sur l'assurance de l'identité : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=30678

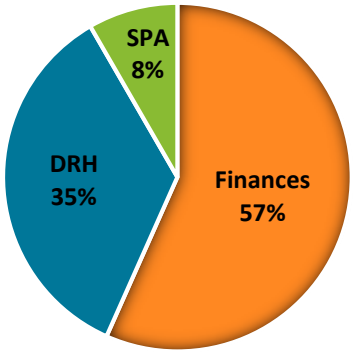

Figure 1 : Proportion de processus opérationnels de niveau d'assurance 2 utilisant des signatures numériques relevant de la direction. DGRH = Direction générale des ressources humaines; SPA = Services professionnels et d'affaires

Approche et méthodologie

La vérification a été effectuée conformément aux normes de l'Institute of Internal Auditors (IIA) et aux Normes relatives à la vérification interne au sein du gouvernement du Canada, comme l'exige la Politique sur l'audit interne du Conseil du Trésor (CT).

Des procédures et des essais de vérification fondés sur le risque ont été mis au point et définis dans le cadre d'un programme de vérification officiel et ont été utilisés pour évaluer les pratiques du CNRC par rapport aux exigences législatives et aux lignes directrices en place. Le programme de vérification comprenait les procédures de vérification suivantes :

- Réalisation d'entretiens avec les principaux intervenants (c'est-à-dire les responsables de processus opérationnels);
- Examen de la documentation pertinente, notamment les documents-cadres, les politiques, les directives, les orientations, les rapports et le matériel de formation;
- Détermination et examen des principaux processus et procédures d'ordre opérationnel en place;
- Échantillonnage et examen de documents signés numériquement;
- Examen et analyse de l'évaluation et de la méthodologie des transactions du CNRC.

Une définition détaillée des critères est présentée à l'annexe A.

3.0 Résultats de la vérification et recommandations

Chaque section ci-dessous présente un résumé des conclusions étayé par des observations détaillées, une description du risque et de l'incidence, ainsi que des recommandations pour aborder les domaines à améliorer.

3.1 Gouvernance et stratégie

Constatations générales

On a constaté dans le cadre de la vérification que la directive sur l'autorisation numérique a été créée et approuvée par la chef de la direction financière. La directive était conforme aux orientations du CT. Les procédures et les normes qui définissent les techniques et les plateformes à utiliser dans l'ensemble du CNRC ont été documentées et communiquées. Le Comité de gestion des risques infotechnologiques (CGRI) a révisé sur une base périodique la directive, les procédures et les normes (la dernière fois en 2021) afin de s'assurer qu'elles sont adaptées et complètes pour régir la mise en œuvre des signatures numériques par le CNRC.

Face à la transition rapide vers le travail à distance, le CNRC a soutenu efficacement les activités opérationnelles en élaborant une directive intérimaire sur l'autorisation numérique approuvée et largement diffusée, ainsi que des outils et des conseils à l'appui. L'élaboration de la directive a commandé la participation d'entités clés, notamment d'un groupe de travail composé de responsables opérationnels qui ont fourni des informations spécifiques sur les niveaux de risque avec lesquels compose leur CDP (pour centre de recherche, direction ou Programme d'aide à la recherche industrielle - PARI), le CGRI et le Comité de gestion de la sécurité (CGS).

Le CGRI a recommandé l'approbation de la directive intérimaire sur l'autorisation numérique à la chef de la direction financière en avril 2020, à la suite de discussions sur la nécessité d'utiliser les signatures numériques dans le cadre du travail à distance. La directive actualisée a été présentée au CGS à des fins d'approbation en septembre 2021.

La vérification a révélé que les rôles et les responsabilités étaient documentés et communiqués à tous les intervenants, en particulier au personnel qui gère et exécute les tâches liées aux autorisations numériques. On a également constaté que les autres intervenants concernés avaient été informés et connaissaient leurs rôles, responsabilités et obligations de rendre compte dans l'exercice de cette tâche. On a constaté que cette façon de faire offrait de la clarté et permettait la bonne exécution des rôles et des responsabilités par les responsables de processus opérationnels pour assurer la validation des signatures numériques par les responsables et par les cadres et les gestionnaires ayant des pouvoirs délégués et pour garantir que les documents numériques sont conservés dans un dépôt approuvé du CNRC. La directive fait maintenant état du rôle des responsables de processus opérationnels de sorte que les responsables de la validation de l'autorisation numérique suivent les étapes requises pour garantir l'authenticité d'une signature numérique.

Avant d'adopter les autorisations numériques, des séances d'information ont été organisées, et certaines étaient adaptées à des groupes particuliers. On a constaté dans le cadre de la vérification que les séances d'information étaient ouvertes à tous les employés du CNRC et que les participants avaient la possibilité de poser des questions. La vérification a également révélé que le CNRC s'emploie de façon proactive à promouvoir la sensibilisation et l'éducation par l'entremise d'un éventail d'activités au moyen de MaZone et d'annonces.

Recommandation

Aucune recommandation.

3.2 Gestion des risques

Constatations générales

Les responsables opérationnels réunis au sein d'un groupe de travail ont établi des niveaux d'assurance minimum pour différentes activités et transactions opérationnelles. Les niveaux d'assurance ont permis de définir une approche fondée sur les risques pour appliquer les différents types d'autorisations numériques en place en cas de compromission d'une autorisation (c'est-à-dire perte d'intégrité des données, abus de pouvoir, etc.) Pour déterminer un niveau d'assurance de 2, des signatures numériques peuvent être utilisées. Suivant l'évaluation terminée et la détermination du niveau d'assurance, des contrôles procéduraux ont été mis en place.

Le groupe de travail sur l'autorisation numérique a élaboré la directive intérimaire sur l'autorisation numérique afin d'établir le format numérique comme méthode privilégiée pour autoriser et approuver les transactions opérationnelles du CNRC, en conformité avec le document Orientation du gouvernement du Canada sur l'utilisation des signatures électroniques. Le groupe de travail était composé de responsables de processus opérationnels possédant de l'expertise dans leurs CDP et en mesure de déterminer avec précision les risques liés aux divers processus opérationnels. Les responsables des processus opérationnels ont évalué chaque activité et transaction dans le cadre d'un groupe de travail, avant la transition vers l'autorisation numérique, afin de déterminer le niveau d'assurance approprié et le type de signature requis.

Pour chaque processus ou activité d'ordre opérationnel, les formulaires et les instructions connexes ont été examinés et mis à jour si nécessaire pour intégrer les signatures numériques. De plus, le groupe de travail a déterminé le niveau d'assurance minimum nécessaire pour exécuter correctement une transaction. L'évaluation des niveaux d'assurance tient compte de l'incidence des menaces, comme la perte d'intégrité des données, la fraude potentielle, etc. Le niveau d'assurance requis pour une autorisation numérique dicte le niveau d'assurance requis pour l'authentification de l'utilisateur et des justificatifs d'identité. Il est ressorti de la vérification que les processus ou activités clés nécessitant une signature numérique avaient un niveau d'assurance défini en fonction des directives du CT.

Recommandation

Aucune recommandation.

3.3 Supervision et suivi

Constatations générales

Bien que les employés aient reçu des instructions de validation des signatures numériques, la vérification a démontré un manque de clarté chez les utilisateurs interrogés sur la manière et le moment de valider les signatures numériques. Il faut mettre en place un mécanisme de contrôle officiel pour garantir que les responsables opérationnels valident les signatures numériques, comme le prévoit la directive. La vérification a par ailleurs montré que les documents signés de façon numérique n'étaient pas systématiquement sauvegardés dans un dépôt officiel, comme l'exige la Politique de gestion de l'information du CNRC.

La surveillance de l'environnement de contrôle interne est de la plus haute importance compte tenu de ces changements importants dans les méthodes de signature des documents par les employés. Des évaluations fréquentes doivent être réalisées de concert avec les responsables des contrôles de sorte que les modifications apportées aux processus ne rendent pas les contrôles inefficaces. Les lacunes relevées dans les contrôles internes doivent être abordées de manière proactive afin de donner aux responsables opérationnels la possibilité d'y remédier.

Les signatures numériques, qui exigent qu'un employé saisisse des informations d'identification avant de signer, par l'intermédiaire d'Entrust, renforcent l'intégrité d'une signature et sont souvent horodatées. Les signatures numériques peuvent également « verrouiller » le document, en interdisant toute modification du document signé. Toutefois, même dans le cas des signatures numériques, il est possible d'éviter la nécessité d'une authentification d'Entrust si les signataires émettent eux-mêmes leurs signatures numériques. Il existe également un risque que les signatures soient modifiées ou supprimées après la modification d'un document. La possibilité de soumettre une signature non valide augmente considérablement le risque de transactions non valides au sein de l'organisation et affaiblit l'environnement de contrôle. Les responsables de processus opérationnels doivent donc faire preuve de diligence pour assurer la validation des signatures numériques dans leurs CDP.

Quel que soit l'outil utilisé pour signer numériquement des documents, tous les documents signés doivent être traités comme des enregistrements ayant une valeur opérationnelle, ne doivent pas être modifiés et doivent être gérés conformément à la Politique de gestion de l'information du CNRC. Les documents signés doivent être stockés dans un dépôt approuvé par le CNRC, approprié au type de document. On s'attendait à ce que des contrôles de sécurité de l'intégrité des systèmes et des informations soient en place pour protéger l'intégrité des transactions électroniques et des enregistrements associés. On a observé des cas où des documents signés numériquement n'étaient pas stockés conformément à la Politique de gestion de l'information du CNRC, comme l'exige sa directive sur l'autorisation numérique.

Sur la base des entretiens menés, la vérification a permis de déterminer que les employés enregistrent parfois des documents sur leurs ordinateurs de travail dans leurs dossiers ou sur des disques durs externes. Ils peuvent procéder de cette façon, ou enregistrer leurs

documents dans DocZone[3], ce qui génère des copies en double. Cela peut prêter à confusion lorsqu'il s'agit de déterminer quelle est la version finale d'un document signé, laquelle doit pouvoir être récupérée sur demande pour une piste de vérification. Une gestion appropriée de ces ressources d'information exige que tous les employés du CDP déterminent systématiquement si l'information a une valeur opérationnelle ou durable et appliquent des pratiques de conservation appropriées. Il est possible que l'information stockée à l'extérieur des dépôts officiels (p. ex. DocZone) ne soit pas gérée adéquatement, ce qui, le cas échéant, nuit à la capacité du CNRC d'indexer, de rechercher, d'extraire, de conserver et d'éliminer l'information conformément à la tenue des dossiers du CT.

Recommandation

1. La vice-présidente des Services corporatifs et chef de la direction financière devrait mettre en œuvre un régime de surveillance axé sur les risques afin de contrôler la conformité aux exigences de la directive pour les processus opérationnels respectifs, y compris la validation des signatures numériques et l'assurance de la conservation des documents numériques dans un dépôt numérique approuvé du CNRC.

   [Priorité : **modérée**]

[3] DocZone : Dépôt officiel du CNRC pour les documents à valeur opérationnelle.

Annexe A : Critères de vérification

Les critères ci- après ont été utilisés pour évaluer la gestion des autorisations numériques au CNRC.

Premier secteur d'intérêt – Gouvernance et stratégie : Des structures et des processus de gouvernance ont été établis et mis en œuvre pour permettre une conception et une exécution efficaces de l'utilisation de l'autorisation numérique.

1. Les rôles, les responsabilités et les obligations de rendre compte sont documentés, attribués et communiqués aux cadres supérieurs et aux principaux intervenants et fonctionnent comme prévu.
2. Conformément aux politiques, aux directives et aux orientations, le CNRC a élaboré, approuvé, communiqué et mis à jour une directive sur l'autorisation numérique avant sa mise en œuvre.

Deuxième secteur d'intérêt – Gestion des risques : Le CNRC a mis en place des régimes pour évaluer et atténuer les risques liés aux transactions et aux activités opérationnelles.

1. On mène une évaluation des activités et des processus d'ordre opérationnel avant de procéder à l'autorisation numérique afin de déterminer lesquels doivent être approuvés pour l'autorisation numérique.
   Les documents signés numériquement sont stockés conformément à la Politique de gestion de l'information et des données et à la directive sur l'autorisation numérique du CNRC.

Troisième secteur d'intérêt – Surveillance et contrôle : Le CNRC a mis en place des régimes de surveillance et de contrôle appropriés pour assurer une utilisation adéquate de l'autorisation numérique.

1. Les responsables des processus opérationnels chargés de valider les autorisations numériques ont suivi les étapes requises pour garantir l'authenticité des signatures numériques.
2. Les employés ont été formés pour utiliser l'autorisation numérique et disposent des outils nécessaires pour valider les signatures numériques.

Annexe B : Plan d'action de la direction

Degré de priorité des recommandations	
Élevé	Mise en œuvre recommandée dans un délai de six mois afin de réduire le risque que des événements potentiels à probabilité ou à incidence élevée compromettent l'intégrité des processus de gouvernance, de gestion des risques et de contrôle du CNRC.
Modéré	Mise en œuvre recommandée dans l'année qui suit afin de réduire le risque que des événements potentiels compromettent l'intégrité des processus de gouvernance, de gestion des risques et de contrôle du CNRC.
Faible	Mise en œuvre recommandée dans l'année qui suit afin d'adopter les meilleures pratiques ou de renforcer l'intégrité des processus de gouvernance, de gestion des risques et de contrôle du CNRC.

Recommandation	Plan des mesures correctives de la direction	Date de mise en œuvre prévue et responsable du CNRC
1. La vice-présidente des Services corporatifs et chef de la direction financière devrait mettre en place un régime de surveillance axé sur les risques afin de contrôler la conformité aux exigences de la directive pour les processus opérationnels respectifs, y compris la validation des signatures numériques et l'assurance que les documents numériques sont conservés dans un dépôt numérique approuvé du CNRC. [Priorité : **modérée**]	Le plan d'audit axé sur les risques des contrôles internes en matière de rapports financiers (CIRF) et des contrôles internes en matière de gestion financière (CIGF) comprend tous les processus opérationnels clés. Par conséquent, l'équipe de surveillance financière des services financiers et d'approvisionnement intégrera la validation des signatures numériques et veillera à ce que les documents numériques soient conservés dans un dépôt numérique approuvé du CNRC dans le cadre du plan d'évaluation. Les résultats de	D'ici le 31 mars 2022, un rappel sera envoyé à tous les responsables opérationnels à propos de leurs responsabilités à l'égard de la directive sur l'autorisation numérique, et celui-ci mettra l'accent sur les points suivants : • Établir, documenter et partager les outils numériques acceptés pour chaque type de transaction ou processus d'ordre opérationnel, y

Recommandation	Plan des mesures correctives de la direction	Date de mise en œuvre prévue et responsable du CNRC
	l'évaluation sont validés et font l'objet de discussions avec les responsables des processus opérationnels qui, à leur tour, fournissent un plan de gestion des mesures. Ces résultats sont également communiqués chaque année dans les états financiers ministériels. De plus, la validation des signatures numériques a été intégrée au processus de vérification des paiements prévu à l'article 33.	compris l'endroit où les documents numériques doivent être conservés; • Veiller à ce que les responsables de la validation des autorisations numériques suivent les étapes requises pour garantir l'authenticité des signatures numériques. Des procédures de validation supplémentaires seront intégrées à la stratégie d'essai des CIRF et des CIGF à compter de l'exercice 2022-2023. Directrice, Opérations comptables, Services financiers et d'approvisionnement