RAPPORT SUR LES TECHNOLOGIES PERMETTANT DE VOTER D'AUTRES FAÇONS

Appendice 5

Étude de cas sur le vote en réseau

Elections Ontario

Elections
Ontario

51, promenade Rolark
Toronto (Ontario)
M1R 3B1

1 888 668 868
ATS: 1 888 292 2312
info@elections.on.ca
elections.on.ca

ISSN 978-1-4606-2019-9 (PDF)

Table des matières

RÉSUMÉ

CONTEXTE

VISION:

En vertu de la *Loi électorale*, il incombe à Élections Ontario de mener une étude sur les modes de scrutin de remplacement et de présenter un rapport sur la question d'ici juin 2013. Dans le cadre de sa stratégie d'innovation, Élections Ontario a décidé d'axer cette étude sur les technologies de vote en réseau et, sous réserve de la faisabilité du projet, de procéder à une évaluation lors d'une élection partielle en 2012. L'étude de cas analyse la pertinence de recourir à ces technologies en Ontario et évalue la faisabilité d'un projet pilote dans les délais impartis.

POSSIBILITÉ À EXPLOITER:

Le vote en réseau est un mode de scrutin et de dépouillement par voie électronique qui repose sur la transmission des bulletins de vote et des suffrages par téléphone, par réseau informatique privé ou par Internet. Comme c'est le cas dans d'autres territoires de compétence, le vote en réseau peut s'avérer bénéfique pour Élections Ontario, dans la mesure où il permet de faciliter le processus de vote et d'améliorer l'accessibilité pour les électeurs handicapés grâce aux options proposées en complément des bulletins de vote sur papier.

OBJET DE LA PRÉSENTE ÉTUDE DE CAS:

Dans la lignée de l'engagement pris par le directeur général des élections en faveur de la modernisation du processus électoral en Ontario, cette étude présente les avantages, évalue les risques et estime les coûts inhérents à un projet pilote sur le vote en réseau.

OBJET DU PROJET PILOTE:

Ce projet pilote visera quant à lui à évaluer la capacité recommandée de la solution choisie aux fins d'étayer les principes d'Élections Ontario. L'évaluation étant prévue dans le cadre d'une élection partielle avec la participation réelle des électeurs, l'approche recommandée doit tenir compte des facteurs de risque et de complexité du vote en réseau dans un environnement concret.

AVANTAGES:

Cette initiative permettra tout de même à Élections Ontario d'obtenir un ensemble de résultats mesurables et de présenter à l'Assemblée législative, en 2013, un rapport fondé sur une étude exhaustive menée lors d'une élection officielle. Le projet pilote donnera l'occasion à Élections Ontario de démontrer l'efficacité de ses stratégies de gestion des risques, de mesurer le taux d'utilisation et l'acceptation par les électeurs des modes de scrutin en réseau et d'évaluer la capacité technologique nécessaire à l'échelle d'une élection générale.

D'après les données de recherche, une vaste proportion de la population ontarienne est favorable à la mise en œuvre de modes de scrutin de remplacement, et cette constatation est confirmée par le recours accru au vote par Internet et par téléphone observé récemment à l'échelon municipal. Ces tendances, combinées à la forte pénétration d'Internet en Ontario, offrent une possibilité de mener un essai grandeur nature sur le vote en réseau, d'évaluer ce mode de scrutin sous tous ces aspects dans le cadre d'une élection et de déterminer la pertinence de sa mise en œuvre lors d'une élection générale.

CONTRAINTES ET PRINCIPES

ÉCHÉANCIER:

Dans l'optique de présenter son rapport à l'Assemblée législative à la fin du premier semestre 2013, Élections Ontario prévoit de terminer son évaluation en 2012. La tenue des élections partielles étant impossible à anticiper, le projet pilote d'Élections Ontario doit être prêt le plus tôt possible en 2012 : c'est la contrainte principale.

CONTRAINTES LIÉES AU PROCESSUS ET À LA COMPLEXITÉ DE MISE EN ŒUVRE :

Pour tenir ce calendrier et inscrire du mieux possible ce projet pilote dans la stratégie d'Élections Ontario, les contraintes suivantes doivent également être prises en compte :

- Réduire au maximum les besoins d'intégration avec les systèmes et processus électoraux existants, en tenant compte en particulier des points d'intégration ayant trait à la liste des électeurs et à la communication des résultats;
- Limiter au maximum l'impact sur l'organisation, notamment tout changement éventuel affectant les processus, le personnel ou la configuration des systèmes;
- Proposer les modes de scrutin en réseau en complément des bulletins de vote sur papier;
- Opter de préférence pour l'adoption d'un mécanisme autonome d'authentification des électeurs, et non pour l'intégration et l'exploitation d'un système d'authentification tiers;
- Proposer le vote en réseau pendant la période de vote par anticipation, mais pas le jour du scrutin;
- Assurer l'accessibilité des interfaces en vue de satisfaire à la norme récemment mise en œuvre avec les dispositifs accessibles servant au marquage des bulletins de vote.

PRINCIPES:

Étant donné que les modes de scrutin en réseau seront mis à l'essai dans le cadre d'une élection officielle, l'adoption de certains principes a directement conduit à écarter diverses options et orienté l'élaboration de l'approche recommandée. Voici la liste de ces principes électoraux fondamentaux :

1. Accessibilité
2. Un électeur, un vote
3. Authentification des électeurs et autorisation du vote
4. Prise en compte des suffrages exprimés par des électeurs admissibles uniquement
5. Vérifiabilité au cas par cas
6. Confidentialité
7. Validation des résultats
8. Disponibilité du service.

La section 3 de l'étude de cas donne une description complète de chaque principe.

EXAMEN DES TRAVAUX DE RECHERCHE

NOTATION ET ÉVALUATION:

À l'issue de l'examen des modes de scrutin en réseau mis en œuvre dans d'autres territoires de compétence et des résultats de la consultation préliminaire menée auprès des parties prenantes, sept mécanismes fondamentaux de vote en réseau et six moyens d'authentification des électeurs ont été identifiés. Après recoupement de ces options, la faisabilité de dix scénarios de vote en réseau a été établie. Ces derniers ont fait l'objet d'une évaluation portant sur leur capacité à étayer les principes électoraux d'Élections Ontario et sur les facteurs de coût, de complexité et de commodité associés à chacun.

LISTE DES QUATRE SCÉNARIOS RETENUS:

Parmi ces dix scénarios, quatre ont été retenus en vue de mener un projet pilote lors d'une élection partielle, en raison de leur capacité à étayer les principes d'Élections Ontario :

1. Vote sur site, par ordinateur, avec authentification supervisée;
2. Vote sur site, par téléphone, avec authentification supervisée;
3. Vote à distance, par ordinateur, reposant sur une authentification par mot de passe;
4. Vote à distance, par téléphone, reposant sur une authentification par mot de passe.

Ces quatre propositions ont été soumises à la direction d'Élections Ontario qui, après examen, a recommandé la réalisation d'une analyse plus approfondie pour identifier les options de mise en œuvre les plus viables dans le cadre du projet pilote.

APPROCHE RECOMMANDÉE

ACQUISITION D'UNE SOLUTION DISPONIBLE SUR LE MARCHÉ :

Il est recommandé de procéder à l'acquisition, à la personnalisation et au déploiement d'une solution de vote en réseau disponible sur le marché (COTS) qui sera utilisée par Élections Ontario lors d'une élection partielle en 2012. À cette fin, un fournisseur doit être choisi d'ici octobre 2011 et la solution doit être prête en vue d'un déploiement en 2012.

DÉPLOIEMENT DES MODES DE SCRUTIN EN RÉSEAU À DISTANCE UNIQUEMENT :

Le modèle recommandé permet de proposer aux électeurs une gamme élargie d'options plus pratiques, tout en satisfaisant aux exigences inhérentes à la sécurité et à l'intégrité. Il prévoit la mise en œuvre des modes de scrutin suivants pendant la période de vote par anticipation, en complément des bulletins de vote sur papier :

1. système de vote à distance par Internet reposant sur une interface Web compatible avec les technologies d'aide au vote;
2. système de vote à distance par téléphone proposé aux électeurs n'ayant pas accès à Internet et rencontrant des difficultés à se rendre en personne sur leur lieu de vote.

APPROCHE D'ENSEMBLE :

Les modes de scrutin sur site retenus lors des travaux de recherche ont été écartés après analyse détaillée. Le mode de scrutin sur site par téléphone présente plusieurs risques et pose des problèmes en matière d'accessibilité et de confidentialité liés à la gestion de l'authentification des électeurs. Le vote sur site par ordinateur présente des avantages marginaux en termes d'accessibilité et de commodité et augmente considérablement la complexité du processus pour Élections Ontario.

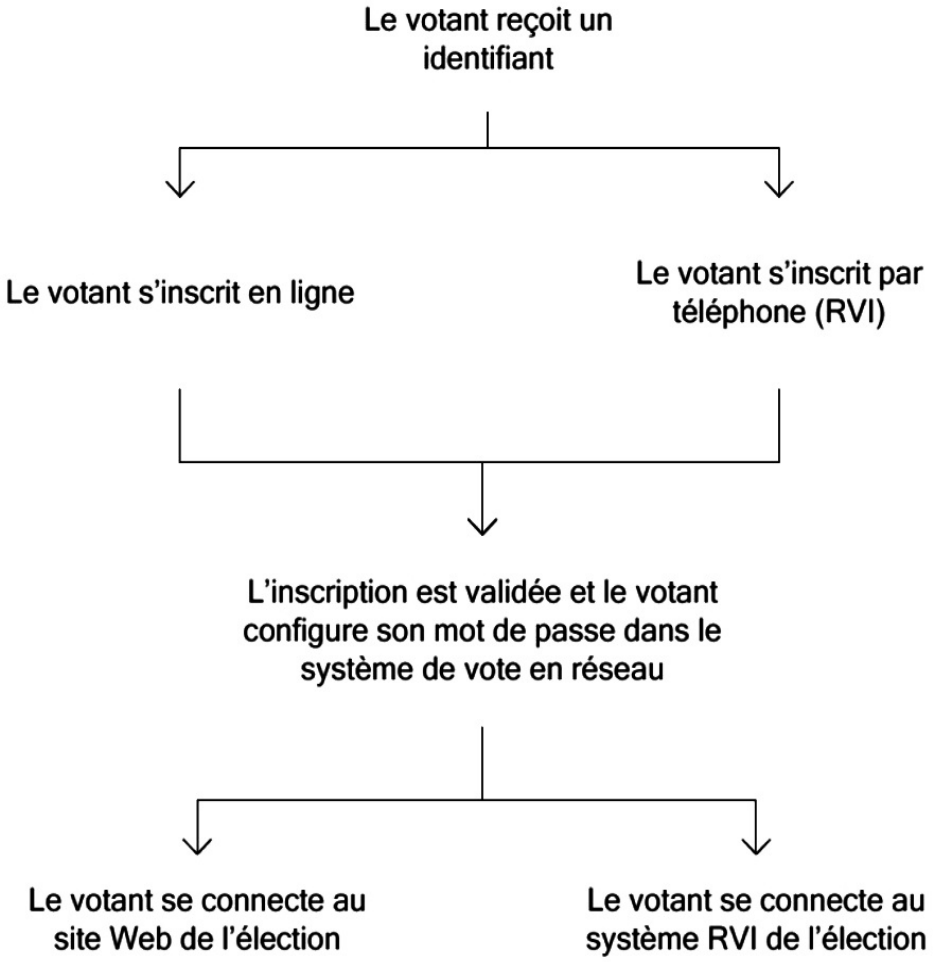
Par conséquent, l'approche recommandée consiste à mettre à l'essai les modes de scrutin à distance, par téléphone et par ordinateur. Tous les électeurs recevront un numéro d'identification par courrier sécurisé et ceux qui désirent utiliser les options de vote en réseau devront s'inscrire à l'avance. Après leur inscription, les électeurs auront la possibilité de voter par Internet ou par téléphone pendant la période de vote par anticipation. Le processus se déroule de la façon exposée ci-dessous.

- Le recours à un document d'identification émis par le gouvernement pour confirmer les déclarations d'identité des électeurs s'avère la méthode la plus sécurisée. Cependant, Élections Ontario a uniquement accès aux données des permis de conduire et, dans ce cas, les électeurs non détenteurs d'un permis de conduire ne peuvent pas s'inscrire via le processus ordinaire. Élections Ontario peut alors décider de privilégier l'accessibilité plutôt que la sécurité.
- Un processus d'inscription reposant sur une forme moins sécurisée de renseignements à caractère personnel (adresse et date de naissance), mais qui introduit un avantage marginal en matière de sécurité grâce à l'envoi d'un second courrier, permettrait à tous les électeurs de l'Ontario d'accéder au même processus. Élections Ontario doit également accepter le fait que cette option, certes plus accessible, rallonge les délais du processus et rend ainsi le vote en réseau plus complexe — ce qui peut s'accompagner d'une baisse de l'utilisation générale et réduire par là même la taille de l'échantillon sur lequel se fondera le rapport présenté à l'Assemblée législative en 2013.

INSCRIPTION ET AUTHENTIFICATION :

1. Les électeurs reçoivent un courrier d'inscription pour le vote en réseau comportant un identifiant numérique sécurisé personnel (ID d'électeur) et des instructions d'accès au site Web d'inscription pour le vote en réseau à distance.
2. Les électeurs qui optent pour le vote en réseau à distance se rendent sur le site Web et saisissent leur ID d'électeur et leur date de naissance afin de s'inscrire. Pour plus de sécurité, le numéro du permis de conduire peut être utilisé pour vérifier leur identité. Un second courrier peut également être envoyé à ce stade pour fournir à l'électeur un second numéro d'identification personnel (NIP) sécurisé avant de passer à l'étape suivante.
3. Après l'authentification, le système valide la qualité d'électeur de chacun et demande la configuration d'un mot de passe sécurisé à utiliser au moment du vote. Éventuellement, les électeurs n'ayant pas facilement accès à Internet peuvent appeler un numéro sans frais pour mener à bien la même procédure via une interface de réponse vocale intégrée (RVI) qui se connecte au même système dorsal.
4. Dès l'ouverture de la période de vote par anticipation, les électeurs inscrits pour le vote à distance peuvent se connecter au site Web ou au système RVI de l'élection à l'aide de leur ID d'électeur et de leur mot de passe.

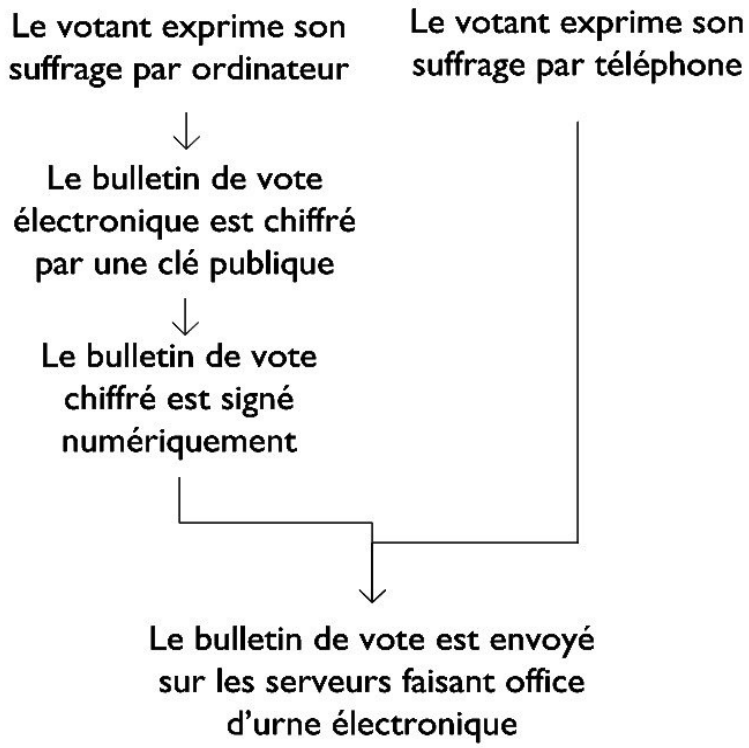
INSCRIPTION ET AUTHENTIFICATION



VOTE:

5. Une fois qu'un électeur a été authentifié sur le site Web de l'élection, il peut exprimer son suffrage en sélectionnant le candidat de son choix à l'écran. Les électeurs votant par téléphone feront leurs sélections via un système de menu automatisé. La facilité d'emploi et l'accessibilité de ces deux options doivent être optimisées afin d'offrir la meilleure expérience possible aux utilisateurs.
6. Après avoir voté par l'un de ces moyens, l'électeur est rayé de la liste des électeurs et reçoit un accusé de réception qui lui permettra de vérifier la prise en compte de son suffrage dans les résultats finaux de l'élection.
7. La liste des électeurs peut être gérée dans le cadre d'un processus en ligne en temps réel pour éviter l'éventualité d'un double vote via différents modes de scrutin et maintenir à jour le système de vote en réseau en fonction des révisions. Il serait aussi possible de cantonner les électeurs aux modes de scrutin à distance une fois leur inscription effectuée afin d'éviter tout risque de double vote.

VOTE

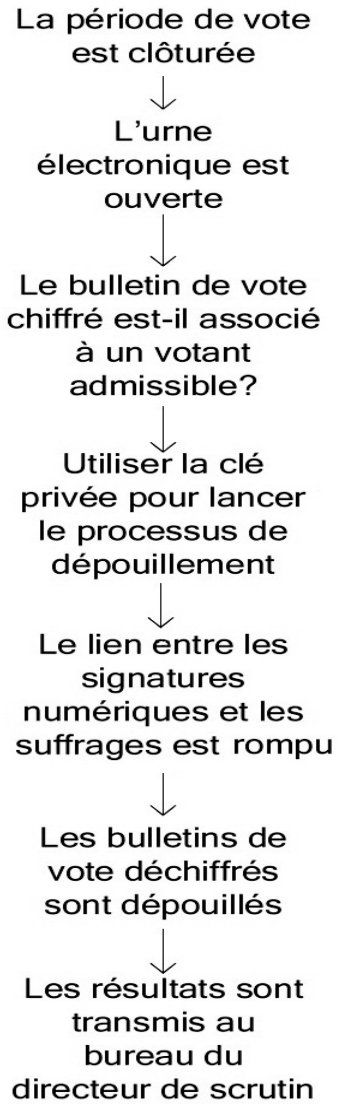


8. Une fois le suffrage exprimé par téléphone ou par ordinateur, le bulletin de vote électronique est archivé dans un environnement serveur sécurisé régi par des mesures de sécurité physiques et logicielles strictes et répondant à des exigences draconiennes en matière de disponibilité et de performance.
9. Ce bulletin de vote fait l'objet d'un chiffrement sécurisé empêchant la lecture de son contenu tant qu'il est archivé dans l'urne électronique.

COMPILATION:

10. À la fin de la période de vote, les urnes électroniques sont transférées dans un environnement isolé et sécurisé en vue du dépouillement.
11. Avant le déchiffrement, le système vérifie que tous les bulletins de vote contenus dans les urnes ont été « déposés » par des personnes ayant les qualités requises pour voter.
12. Les bulletins de vote sont déchiffrés par les membres autorisés au sein du personnel d'Élections Ontario, chacun d'entre eux étant en possession d'une partie de la clé nécessaire au déchiffrement.
13. Après le déchiffrement, les bulletins de vote ne peuvent pas être associés à un électeur.
14. Le système compte les bulletins valides et communique les résultats combinés du vote en réseau au directeur du scrutin, qui les inclut au décompte officiel.

Compilation



VÉRIFICATION:

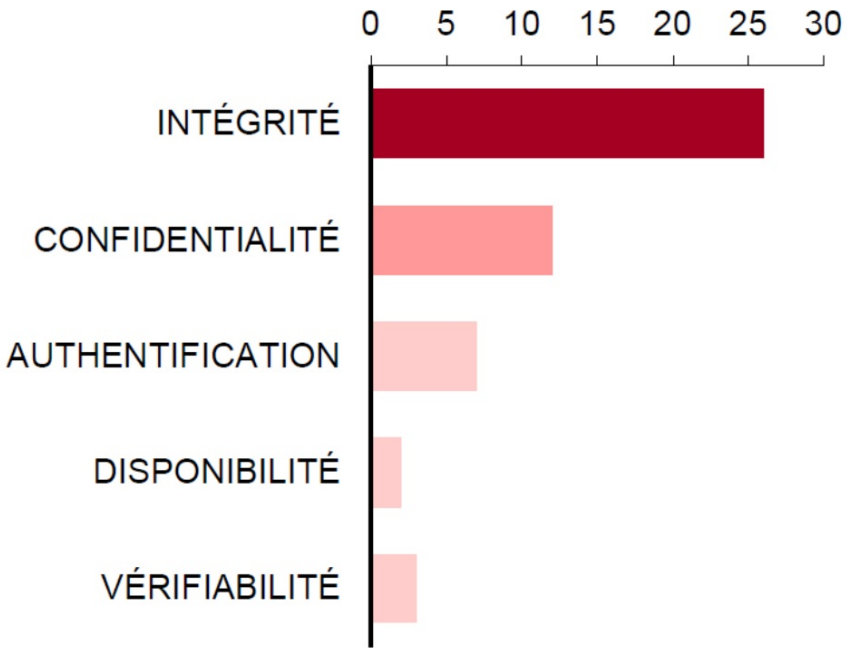
15. Le système doit permettre au conseil de gestion du vote en réseau de procéder à un nouveau déchiffrement et à une nouvelle compilation, le cas échéant, sous la supervision de vérificateurs indépendants.
16. Le système doit permettre aux vérificateurs indépendants de procéder à un nouveau décompte, en parallèle de la liste certifiée des bulletins de vote déchiffrés. Les vérificateurs doivent être en mesure de travailler à partir des bulletins de vote déchiffrés et d'obtenir des résultats traduits en clair susceptibles d'être comparés à ceux générés par le système.
17. Le système doit permettre aux vérificateurs indépendants de vérifier et de certifier l'intégrité et l'authenticité des composantes du système utilisées dans le traitement des urnes électroniques, y compris l'authenticité des logiciels, l'intégrité du système, l'intégrité et l'authenticité des fichiers journaux générés, etc.

ÉVALUATION DES RISQUES

Bien que cette approche soit recommandée en raison de sa capacité à étayer les principes d'accessibilité, d'intégrité et de sécurité, certains risques persistent. Un modèle de scrutin en réseau fondé sur l'association des options de vote par ordinateur et par téléphone est susceptible d'être vulnérable dans plusieurs domaines, en particulier sur le plan de la sécurité.

Comme l'illustre le diagramme ci-après intitulé « Catégories de risques en matière de sécurité », la première catégorie de risque en matière de sécurité concerne l'exactitude des résultats, c'est-à-dire un élément ayant un impact direct sur l'intégrité de l'élection. Les menaces en la matière incluent l'éventualité que les suffrages puissent être modifiés ou supprimés au moment du vote, une fois que les bulletins de vote sont archivés sur le système ou lors du dépouillement.

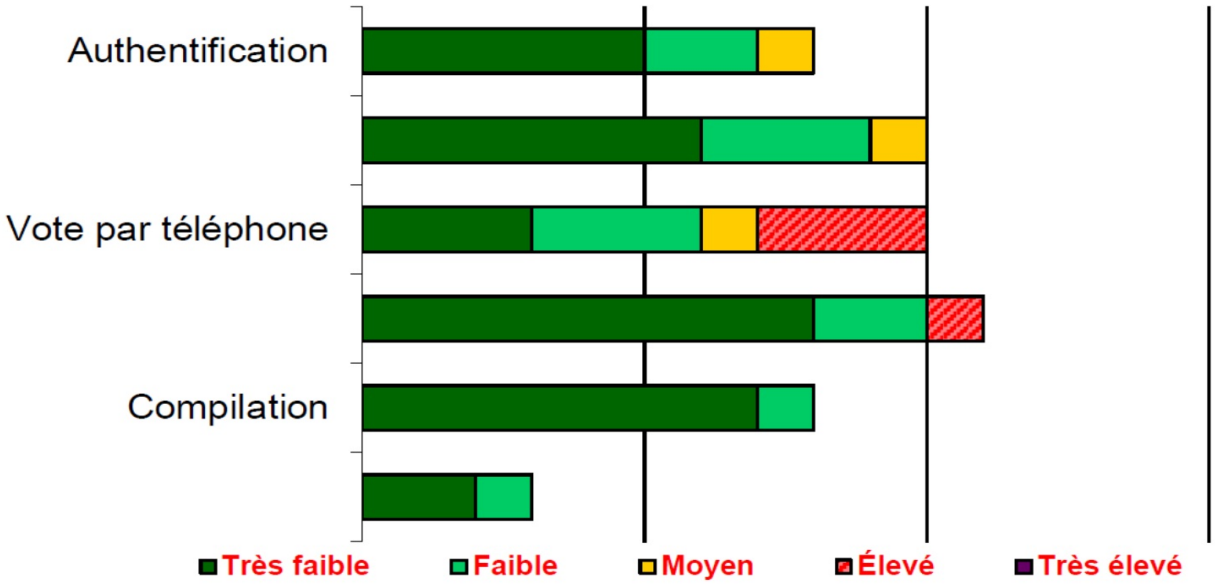
Catégories de risque en matière de sécurité



Ensuite, diverses menaces portant sur la création d'un lien entre l'électeur et le suffrage exprimé peuvent affecter la confidentialité du vote. En outre, si les protocoles d'authentification ne sont pas suffisamment sécurisés, l'identité des électeurs pourrait être usurpée ou le nom de personnes n'ayant pas les qualités requises pour voter pourrait être ajouté à la liste des électeurs. Les risques d'un potentiel déni de service peuvent également compromettre la disponibilité du système pendant le vote, ainsi que les données requises pour assurer la vérifiabilité de l'élection.

Le diagramme qui suit, intitulé « Niveaux de risque résiduel à chaque étape du processus », présente un diagramme ci-contre synthétise l'évaluation des risques en matière de sécurité associés au système de vote en réseau. Il illustre le nombre de menaces potentielles à chaque étape du processus électoral et comporte deux lignes : une pour chaque mode de scrutin. Ce diagramme indique également le niveau de risque résiduel, sous réserve de la mise en œuvre des mesures d'atténuation appropriées.

Niveaux de risque résiduel à chaque étape du processus



Dans la majorité des cas, les menaces peuvent être atténuées de manière à limiter le risque résiduel à un niveau faible, voire très faible. Certains risques restent à un niveau moyen sur des points comme l'authentification par téléphone et le vote sous la contrainte.

La seule étape du processus présentant un risque résiduel élevé concerne le vote par téléphone, en raison des trois menaces majeures suivantes :

- interception du suffrage par un pirate entre l'appel téléphonique et le moment où le bulletin de vote est archivé sur les serveurs sécurisés de l'élection;
- interception des suffrages par un administrateur du système RVI pendant le transit, ce qui est contraire au principe de confidentialité et constitue une publication non autorisée;
- interception et modification des suffrages par un pirate.

Bien que bon nombre des risques techniques inhérents à un mode de scrutin en réseau puissent être atténués grâce au choix de la technologie adaptée en matière de sécurité, un risque persiste quant à la perception de ces options par le public. Bien qu'ils soient minoritaires, certains adversaires farouches du vote en réseau affirment que ce processus est par nature moins fiable, moins sécurisé, voire moins démocratique que les modes de scrutin traditionnels. Une perception négative du public est susceptible de nuire à la mise en œuvre réussie du vote en réseau, mais cette menace peut être atténuée en élaborant une stratégie de communication globale.

CRITÈRES DE RÉUSSITE

1. Le projet pilote doit mettre en œuvre un système qui préserve, preuves à l'appui, une « chaîne de confiance » ininterrompue contrôlant la détention des données de vote. Le système doit permettre aux vérificateurs indépendants de vérifier et de certifier l'intégrité et l'authenticité des composantes du système utilisées dans le traitement des urnes électroniques, y compris l'authenticité des logiciels, l'intégrité du système, l'intégrité et l'authenticité des fichiers journaux générés, etc.

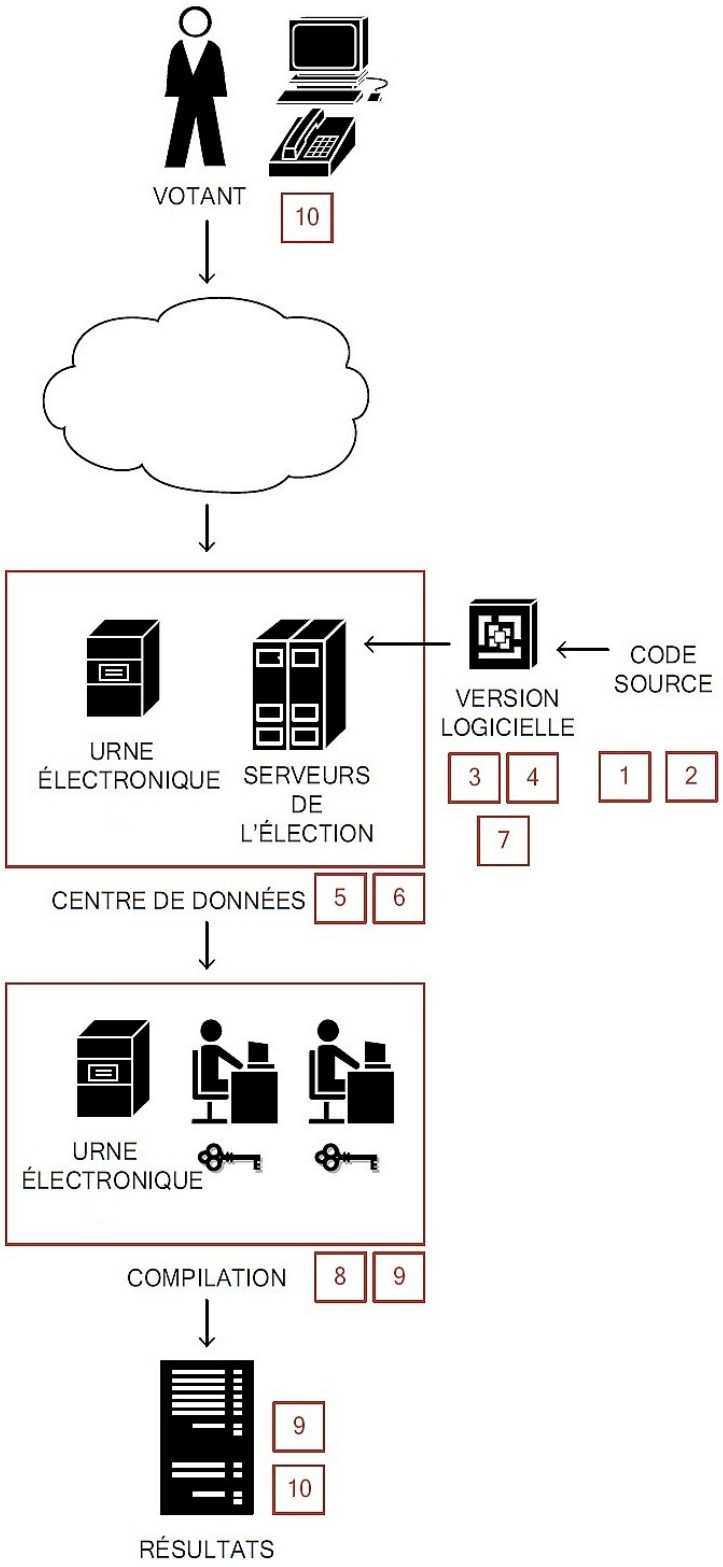
   La réussite et l'intégrité d'une élection reposent sur l'absence de toute possibilité d'altération des bulletins de vote. Dans un système de vote en réseau, les données peuvent être altérées si un code malveillant est installé à un point quelconque de la chaîne de détention des bulletins de vote. Pour prouver l'intégrité de l'élection, Élections Ontario doit être en mesure de démontrer que seuls les parties et les logiciels dûment autorisés ont eu accès aux données des bulletins de vote numériques.

   Si la mise en œuvre du système de vote en réseau ne permet pas à la fois d'établir une chaîne de confiance et de fournir des preuves vérifiables, le processus peut être contesté. Cette chaîne de confiance est le fruit de l'ensemble des mesures suivantes :

   - Vérification du code source permettant de s'assurer qu'aucune opération non prévue ne peut être exécutée.
   - Signature numérique du code source vérifié permettant de protéger son authenticité et son intégrité.
   - Création d'une version fiable du code exécutable en présence des vérificateurs (à partir du code source vérifié).
   - Signature du code exécutable permettant de protéger son authenticité et son intégrité.
   - Déploiement du logiciel exécutable sur un système propre.
   - Sceau électronique associé au système afin de détecter tout ajout ultérieur.
   - Test de cohérence et de précision du système de vote visant à valider son bon fonctionnement.
   - Vérification en continu du système de vote pendant l'élection, via l'examen et la validation des fichiers journaux et d'autres données. Les fichiers journaux doivent être chiffrés afin d'empêcher toute manipulation extérieure.
   - Vérification postélectorale validant le comportement du système après examen des sceaux électroniques et des fichiers journaux protégés.
   - Vérification individuelle par les électeurs prouvant que leurs suffrages ont été pris en compte dans le résultat final (grâce à l'envoi d'accusés de réception spéciaux).

La vérification doit figurer parmi les priorités. Il faut permettre à des vérificateurs indépendants d'étudier le code source, de vérifier la version et le déploiement du logiciel, d'examiner les fichiers journaux du système pendant le scrutin et enfin d'analyser le processus de dépouillement et les résultats.

Chaîn de confiance



2. Une équipe de projet expérimentée doit mener à bien une approche de mise en œuvre efficace s'articulant autour des points suivants :
   - Acquisition d'un système hôte sécurisé hautement disponible;
   - Acquisition d'une solution COTS assurant un niveau élevé de sécurité de bout en bout et dont le fournisseur justifie d'une expérience dans le cadre d'élections officielles à grande échelle;
   - Test approfondi de l'utilisation et des performances;
   - Démonstrations et examen par les parties prenantes;
   - Participation dédiée d'experts du domaine chez Élections Ontario visant à assurer l'adaptation sur mesure de la solution;
   - Consultation suivie visant notamment à élargir le panel des parties prenantes consultées.
3. Pour évaluer la réussite du vote en réseau et fournir un rapport sur la pertinence de recourir à ce type de technologies en Ontario, Élections Ontario devra être capable de mesurer les résultats du projet pilote d'après un ensemble concret d'objectifs définis sur la base des principes fondamentaux du vote en réseau. Cette étude de cas propose des outils d'évaluation et de mesure visant à déterminer le respect de chacun de ces principes.

   Pendant la mise en œuvre du projet, il est indispensable de définir des indicateurs de mesure spécifiques et leurs valeurs cibles. Chaque principe peut être évalué par divers moyens, notamment : sondages postélectoraux, sondages sur l'expérience en ligne, résultats de vérification et surveillance technique.
4. Autre point tout aussi important : Élections Ontario devra parvenir à convaincre le public de la sécurité et de l'intégrité du processus par le biais d'une campagne de sensibilisation détaillée démontrant à la fois qu'il existe des préoccupations légitimes et qu'elles sont prises en compte.

ESTIMATION DES COÛTS DU PROJET PILOTE

MODÈLE RECOMMANDÉ : DEUX MODES DE SCRUTIN À DISTANCE

Le coût estimé d'un projet pilote portant sur les deux modes de scrutin recommandés est établi à 1 745 500 $, environ la moitié de cette somme devant être affectée aux coûts de la solution COTS. Ce chiffre correspond au budget total nécessaire pour personnaliser et mettre à l'essai la solution COTS, obtenir une licence pour 100 000 électeurs à 2 $ par personne, tenir l'élection, procéder au dépouillement et procéder à la vérification de l'intégralité du processus.

Cependant, la majorité de ces coûts ne seront pas renouvelés si une seconde élection partielle est organisée la même année. Le poste budgétaire récurrent le plus important correspond à la solution COTS, c'est-à-dire principalement aux coûts de licence des électeurs et d'assistance pendant l'élection. L'autre dépense récurrente correspond au coût associé à la mise en œuvre du scrutin (approbation et déploiement du système, personnel de soutien et envoi de courriers sécurisés). Par conséquent, en cas de recours au vote en réseau à distance lors d'une seconde élection partielle avec 100 000 électeurs participants, le budget supplémentaire s'élèverait à environ 649 500 $.

Bien qu'il s'avère difficile d'estimer avec précision les coûts inhérents à une élection générale, il est important de noter qu'un facteur clé est susceptible de changer : les frais de licence facturés par un fournisseur de solution COTS ne s'élèveront plus qu'à 0,25 $ par utilisateur. En raison de la diminution des coûts de licence par électeur, les dépenses seraient ventilées de façon plus uniforme entre les postes budgétaires suivants : Solution COTS, Coûts d'emplacement et Déploiement.

Les chiffres présentés dans cette étude se fondent sur une étude de marché et peuvent faire l'objet de variations importantes dans le cadre d'une soumission concurrentielle ou d'une négociation contractuelle. Les coûts réels seront déterminés lors du processus d'achat.

Couts du projet pilote

Couts du projet pilote (vote à distance uniquement)	
Solution COTS	$837 000,00
Coûts du lieu de vote	$0
Infrastructure centrale	$162 000,00
Coûts de déploiement	$217 500,00
Coûts des ressources du projet	$429 000,00
Autres couts dû project	$100 000,00
TOTAL	$1 745 500,00

RECOMMANDATIONS PRINCIPALES

VOTE À DISTANCE UNIQUEMENT :

Le déploiement de modes de scrutin à distance uniquement peut permettre d'atteindre les objectifs du projet pilote. Au vu de la complexité et du coût de déploiement des modes de scrutin en réseau sur site et des bénéfices marginaux offerts en termes d'accessibilité, investir dans cette solution pour le projet pilote ne se justifie pas.

ACCÈS NON UNIVERSEL À L'AUTHENTIFICATION PAR NUMÉRO DE PERMIS DE CONDUIRE :

L'authentification des électeurs est l'un des huit principes fondamentaux que le projet pilote doit étayer. Pourtant, le processus associé est à l'origine de plusieurs risques majeurs en matière de sécurité, notamment du risque d'usurpation d'identité des électeurs. L'atténuation de ces risques repose en partie sur l'intégration de renseignements à caractère personnel dans le processus d'inscription des électeurs, dans le but de confirmer leurs déclarations d'identité. À l'heure actuelle, l'option la plus sécurisée consiste à recourir à un document d'identification émis par le gouvernement, à savoir le numéro de permis de conduire.

Bien que la vérification de l'identité des utilisateurs par ce biais constitue la meilleure solution à ce jour, ce moyen pénalise directement les électeurs se trouvant dans l'incapacité d'obtenir un permis de conduire. Ce compromis peut sembler acceptable dans le cadre du projet pilote, mais Élections Ontario devra tout de même utiliser une forme d'identification plus universelle ou d'autres renseignements à caractère personnel lors des prochaines échéances électorales.

ÉLABORER UN MODÈLE D'AUTHENTIFICATION PLUS UNIVERSEL:

Les possibilités de mise en œuvre d'une méthode d'authentification plus universelle existent et doivent être approfondies. Élections Ontario doit mener simultanément ses recherches dans deux directions :

- l'utilisation d'un renseignement à caractère personnel plus universel que le numéro de permis de conduire pour vérifier l'identité des électeurs lors de leur inscription; et
- l'intégration et l'exploitation d'un mécanisme d'authentification tiers, comme le projet ServiceOntario.

Aux fins du projet pilote, Élections Ontario peut envisager d'instaurer un mode d'inscription moins robuste, mais plus accessible, par exemple, le processus d'envoi par la poste en deux étapes décrit au chapitre 6.

LE PROJET PILOTE DE VOTE À DISTANCE N'IMPLIQUE PAS LA CRÉATION D'UN REGISTRE DU SCRUTIN ÉLECTRONIQUE :

Si le vote en réseau était proposé à la fois à distance et sur site, les menaces créées par la mise à disposition en parallèle de plusieurs modes de scrutin (papier, ordinateur et téléphone) et de différents types d'authentification (physique et mot de passe) mettraient en péril deux principes fondamentaux : la capacité à garantir qu'un seul vote par électeur est pris en compte et la nécessité de compter uniquement les suffrages exprimés par des électeurs admissibles. Pour atténuer ces menaces, il faudrait prévoir un registre du scrutin en ligne mis à jour en temps réel qui gèrerait simultanément le vote en réseau et le mode de scrutin sur papier. En l'absence de registre du scrutin électronique, il serait possible que les électeurs votent deux fois : une fois en ligne et une fois en personne.

Toutefois, en éliminant le vote en réseau sur site, le risque qu'un électeur vote plusieurs fois est réduit et il s'avère plus difficile de justifier la création d'un registre du scrutin électronique, au vu des facteurs de coût et de complexité. Dans ce scénario, le risque peut être contrôlé en autorisant les électeurs inscrits pour le vote en réseau à voter uniquement à distance. Leurs noms n'apparaissant pas sur les registres du scrutin physiques, ces électeurs ne peuvent pas déposer un bulletin de vote sur papier pendant la période de vote par anticipation.

LE VOTE PAR TÉLÉPHONE PRÉSENTE DES RISQUES, MAIS ACCROÎT L'ACCESSIBILITÉ DU VOTE :

Le vote par téléphone présente des risques intrinsèques parmi les plus difficiles à gérer ou à atténuer convenablement. Ces risques découlent du fait que le vote par téléphone utilise une infrastructure impossible à sécuriser de la même façon qu'un réseau informatique. Les lignes téléphoniques publiques ne sont pas sécurisées, ce qui crée des risques sur le plan de la confidentialité. Ensuite, les suffrages ne sont pas chiffrés au sein de l'environnement RVI, où ils peuvent donc être interceptés, lus, voire modifiés. Cependant, l'inclusion du vote par téléphone améliore considérablement l'accessibilité du vote en réseau au sein des segments de la population qui n'ont pas accès à un ordinateur et à Internet ou qui ne sont pas à l'aise avec ces technologies. Ces risques peuvent être atténués dans une certaine mesure, principalement grâce à la sécurisation de l'environnement RVI et au déploiement de systèmes de détection des intrusions. La suppression du vote par téléphone affaiblirait la conformité aux principes du projet, mais permettrait aussi de réduire les risques, les coûts et la complexité.

ÉLECTIONS ONTARIO DOIT CONTRÔLER L'ENVIRONNEMENT HÔTE :

La capacité d'Élections Ontario à contrôler du mieux possible l'environnement de vote en réseau sera un élément capital dans l'instauration et le maintien de la chaîne de confiance. Par conséquent, Élections Ontario doit faire l'acquisition d'un environnement hôte (Web + RVI notamment) en vertu d'un accord distinct du contrat d'achat de la solution COTS, et le fournisseur sélectionné devra préciser en détail ses besoins sur le plan du matériel et de l'infrastructure. Sinon, la demande de propositions (DP) doit stipuler que le serveur hôte est physiquement dédié au projet électoral, afin que les serveurs puissent être scellés en vertu du principe de la chaîne de confiance aux fins d'assurer sa vérifiabilité.

La réussite et l'intégrité d'une élection reposent sur l'absence de toute possibilité d'altération des bulletins de vote. Pour prouver l'intégrité de l'élection, Élections Ontario doit être en mesure de démontrer que seuls les parties et les logiciels dûment autorisés ont eu accès aux données des bulletins de vote numériques. La vérification doit figurer parmi les priorités. Il faut permettre à des vérificateurs indépendants d'étudier le code source, de vérifier la version et le déploiement du logiciel, d'examiner les fichiers journaux du système pendant le scrutin et enfin d'analyser le processus de dépouillement et les résultats.

Lors de la planification du projet pilote, il est conseillé d'intégrer des examens intermédiaires de vérification avant de passer à l'étape suivante du projet de vote en réseau. Une révision des décisions validant ou non la mise en œuvre du projet pilote doit être prévue à la suite de :

- l'approbation de l'étude de cas;
- l'approbation du mandat du projet;
- l'évaluation des réponses à la DP/des fournisseurs – en fonction du coût;
- la réalisation de l' essais d'acceptation par l'utilisateur (EAU), du test de performances du système, de l' évaluation de la menace et des risques/évaluation de l'impact sur la protection de la vie privée (ÉMR/ÉIPVP), et
- l'évaluation de la circonscription électorale concernée par l'élection partielle.

CONCLUSION

L'approche recommandée pour la mise en œuvre du vote en réseau consiste par conséquent à proposer un mode de scrutin par téléphone et un mode de scrutin par Internet lors d'une prochaine élection partielle. La réalisation d'un projet pilote en vertu du modèle général décrit au chapitre 6, mais sans mode de scrutin sur place, permettra de procéder dans le respect des contraintes opérationnelles d'Élections Ontario, des principes électoraux fondamentaux, de l'orientation stratégique et des objectifs définis.

L'organisation d'un projet pilote dans le cadre d'une élection partielle avec élargissement des modes de scrutin proposés aux électeurs grâce aux options de vote en réseau à distance, tout en maîtrisant le budget global et la complexité du déploiement, constituera une base solide et approfondie en vue de l'élaboration du rapport qu'Élections Ontario devra présenter à l'Assemblée législative en 2013. Pour ce faire, le projet pilote doit être structuré de façon que Élections Ontario puisse démontrer si les principes électoraux fondamentaux sont bien étayés, si une bonne gestion des risques peut être appliquée et si le rapport bénéfices/coûts est favorable.

1. CONTEXTE

En vertu de la version actuelle de la loi électorale, il incombe au directeur général des élections de mener une étude sur les modes de scrutin de remplacement et de présenter un rapport sur la question au président de l'Assemblée d'ici le 30 juin 2013. Élections Ontario a décidé que si c'est faisable, l'étude pourrait prendre la forme d'un projet pilote sur les technologies de vote en réseau au cours d'une élection partielle tenue en 2012.

1.1 OBJET DU PRÉSENT DOCUMENT

RECOMMANDATIONS DE MISE EN ŒUVRE

LA PRÉSENTE ÉTUDE DE CAS analyse le vote en réseau et recommande une combinaison de technologies de vote et de mécanismes d'authentification des utilisateurs dont la faisabilité a été évaluée dans le contexte de l'Ontario. Elle utilise les facteurs et les contraintes uniques d'Élections Ontario comme fondement de l'analyse, intègre les résultats de la consultation menée auprès des parties prenantes et d'une analyse détaillée de l'industrie, présente une approche spécifique de mise en œuvre, et comprend une analyse exhaustive des risques.

1.2 LA POSSIBILITÉ

Des recherches effectuées récemment révèlent qu'une vaste proportion de la population voit d'un œil favorable le vote par internet, ce que reflète le mouvement récent vers le vote par internet à l'échelon municipal. Compte tenu du taux élevé d'accès à internet chez les ontariens, l'Ontario pourrait mettre en place un projet pilote de solution de vote en réseau et faire d'Élections Ontario un organisme innovateur.

AVANTAGES

En termes généraux, la technologie de vote en réseau peut faire bénéficier une entité responsable de l'élection de nombreux avantages et de possibilités d'un service amélioré :

- **Facilité de voter :** le vote en réseau procure un autre mode de scrutin en laissant les votants exprimer leur suffrage en tout temps et lieu, notamment les électeurs qui résident ou habitent à l'extérieur de l'Ontario.
- **Accessibilité du vote** : le vote en réseau élargit l'accès pour les votants handicapés ou pour ceux qui peuvent difficilement être présents dans un bureau de scrutin et qui utilisent les dispositifs qui y sont disponibles.

1.3 LES RISQUES

RISQUES POUR LA SÉCURITÉ

Le vote en réseau comporte de nombreux avantages. Cependant, il présente également des risques qui peuvent, s'ils sont mal gérés, mettre en péril l'intégrité d'une élection. Ces dernières années, l'industrie a élaboré des façons d'atténuer les risques techniques et les risques pour la sécurité d'un mode de vote en réseau, mais il subsiste le risque tout aussi probable et pertinent de la perception du public.

RISQUES AU NIVEAU DE LA PERCEPTION DU PUBLIC

Bien que les adversaires les plus virulents au vote en réseau soient en minorité, ils affirment que ce mode de scrutin est intrinsèquement moins fiable, sûr ou démocratique que les modes de scrutin traditionnels. Cette perception pourrait constituer une menace plus grande pour la réussite de la mise en œuvre du vote en réseau que les difficultés techniques possibles.

1.4 MOTEURS DU PROJET

ÉTUDE DE MODES DE SCRUTIN DE REMPLACEMENT

En réaction à l'adoption du projet de loi 231, qui renferme une disposition exigeant que le DGE procède à une étude des modes de scrutin de remplacement et présente un rapport d'ici le 30 juin 2013, Élections Ontario a lancé un projet de recherche sur d'autres modes de vote en réseau. Ce projet est dynamisé par l'engagement du directeur général des élections de moderniser le processus électoral en Ontario au moyen de solutions à la fois conventionnelles et technologiques.

POSSIBILITÉ D'INNOVER

Projet pilote au cours d'une élection partielle

L'article 4.1 de la *Loi électorale*[1] donne à Élections Ontario la possibilité de mettre à l'essai et d'évaluer les solutions de vote en réseau dans une élection officielle et de démontrer si le vote en réseau répondra aux besoins et relèvera les défis de l'électorat de l'Ontario. Un projet pilote appliqué au cours d'une élection officielle devrait permettre de mesurer tout un éventail d'options de vote en réseau en regard des principes de scrutin qu'Élections Ontario doit appliquer. Pour tirer le maximum de la possibilité qu'offre un projet pilote d'élection partielle, il conviendrait d'étudier de nombreux modes de scrutin en réseau à des fins de mise à l'essai et d'évaluation pour valider les technologies et les processus qui pourraient être réalisables à l'échelle d'une élection générale.

1.5 OBJECTIFS DU PROJET PILOTE

Le projet pilote de technologie de vote en réseau permettra à ÉO de s'acquitter de nouvelles responsabilités législatives. Il étudiera les modes de scrutin de remplacement et présentera un rapport sur cette étude au président de l'Assemblée d'ici le 30 juin 2013. Le projet pilote devrait évaluer le vote en réseau comme mode de scrutin de remplacement et non évaluer la solution spécifique ou la plateforme utilisée pour mettre en œuvre le projet pilote. Les objectifs comprennent :

- ***Évaluer*** le vote en réseau comme mode de remplacement qui augmente l'accessibilité et l'utilité pour tous les électeurs.
- Mesurer le ***taux d'utilisation et d'acceptation*** par l'électeur des autres modes de scrutin en réseau et évaluer l'attitude du public.
- Évaluer ***l'adaptabilité*** des autres modes de scrutin en réseau à une élection générale.
- Valider que le vote en réseau protège la ***sécurité et l'intégrité*** de l'équivalent de l'élection standard (sans que ce soit nécessairement identique pour chaque élément).

1.6 DOCUMENTS CONNEXES

Élections Ontario, N*etwork Voting Options Evaluation* (version 2.0); 8 mars 2011.

1.7 HISTORIQUE DU DOCUMENT

- Ébauche présentée au directeur général des élections et à l'équipe de la haute direction le 29 avril.
- Ébauche révisée présentée le 31 mai.

2. CONTEXTE DÉCISIONNEL

Le chapitre qui suit décrit les facteurs qui doivent être pris en compte dans le cadre de l'évaluation et de l'analyse de l'application de la technologie de vote en réseau en Ontario et donne un aperçu des moteurs stratégiques et des contraintes pratiques qui touchent cette initiative.

CONTRIBUTIONS À LA PRISE DE DÉCISIONS

BIEN QUE LA RECHERCHE décrite ci-après aux chapitres 4 et 5 recense un certain nombre de scénarios de vote en réseau qui pourraient être réalisables, des facteurs temporels, financiers, juridiques et démographiques limitent le mode de mise en œuvre des approches et technologies de vote en réseau en Ontario. En outre, des groupes de parties prenantes clés s'intéressent à l'issue de la solution du vote en réseau en Ontario. Le présent chapitre décrit la façon dont les facteurs suivants contribuent au contexte décisionnel :

- l'orientation stratégique d'Élections Ontario;
- les contraintes du projet;
- le public cible;
- l'issue de la consultation auprès des parties prenantes;
- un ensemble d'hypothèses de travail qui ont orienté l'analyse des modes de vote en réseau possibles.

2.1 ORIENTATION STRATÉGIQUE

L'approche de vote en réseau recommandée par cette étude de cas a été évaluée en regard de sa capacité d'appuyer l'orientation stratégique d'Élections Ontario, qui est définie comme une combinaison de la mission, de la vision et des valeurs de l'organisation, de certains moteurs du projet, et des priorités stratégiques d'Élections Ontario.

Mission, Vision et Valeurs

INTÉGRITÉ ET ACCESSIBILITÉ

La mission déclarée d'Élections Ontario consiste à « protéger l'intégrité et l'accessibilité du processus électoral et d'administrer les élections de manière juste et impartiale ». Ces principes d'intégrité, d'accessibilité et de justice sont des valeurs qui complètent les valeurs clés pertinentes de réceptivité, d'innovation et de transparence. Enfin, Élections Ontario a une vision d'« établir la norme de l'excellence du processus électoral » et « d'innover et de faire preuve de leadership dans la définition des points de repère importants pour l'administration des élections »[2].

MOTEURS DU PROJET

La motivation d'un projet pilote potentiel sur le vote en réseau repose sur les trois moteurs suivants :

CHOIX DU VOTANT

- Placer les besoins du votant au premier rang en offrant plus de choix.
- Rendre le vote plus facile et accessible pour tous les Ontariens.
- Établir la norme de l'excellence du processus électoral en continuant d'innover et de faire preuve de leadership dans la définition des points de repère importants pour administrer les élections.

Priorités Stratégiques

Toute méthode de vote en réseau ou combinaison de telles méthodes doit soutenir les priorités stratégiques d'ÉO pour 2008-2011, qui sont les suivantes :

- Tenir le registre permanent des électeurs de l'Ontario et élaborer ses produits.
- Élargir les activités d'éducation et de sensibilisation du public d'ÉO.
- Gérer les activités d'ÉO.
- Protéger l'intégrité du processus électoral.

Aux fins de la présente étude de cas, les priorités 1 et 4 serviront à évaluer l'approche recommandée de mise en œuvre du vote en réseau. En d'autres termes, il doit être établi que l'approche retenue appuie les priorités d'Élections Ontario qui consistent à **élaborer** sa gamme de produits et à protéger l'**intégrité** du processus électoral.

2.2 CONTRAINTES

Il existe toute une série de contraintes pratiques qui limitent l'éventail des options de mise en œuvre possible. La présente section définit ces contraintes selon les catégories suivantes :

- Contraintes législatives
- Contraintes liées au processus
- Contraintes liées à l'échéancier
- Contraintes de coûts
- Contraintes techniques.

D'autres facteurs, comme les contraintes sociodémographiques, font l'objet de sections ultérieures.

Contraintes législatives

RAPPORT SUR LES MODES DE SCRUTIN DE REMPLACEMENT D'ICI JUIN 2013

La contrainte législative principale est que le directeur général des élections de l'Ontario est tenu de « mener une étude des modes de scrutin de remplacement, d'élaborer un rapport sur l'étude et, au plus tard le 30 juin 2013, de présenter le rapport au président de l'Assemblée ». Bien que cette loi offre à Élections Ontario l'occasion de réaliser cette étude de cas, elle limite également Élections Ontario sur le plan de l'échéancier (voir ci-après) et du format de l'évaluation, car l'étude doit être suffisamment exhaustive et concluante pour permettre de présenter un rapport concluant sur la pertinence des modes de scrutin de remplacement en général.

Contraintes liées au processus

RAPPORT FONDÉ SUR UN PROJET PILOTE AU COURS D'UNE ÉLECTION OFFICIELLE

Pour relever les défis de la possibilité de nature législative, Élections Ontario a décidé que l'évaluation du vote en réseau peut, si possible, être effectuée dans le cadre d'un projet pilote au cours d'une élection officielle (vraisemblablement une élection partielle) et non dans le contexte d'un essai théorique; toutefois, pour atténuer les risques prévisibles, Élections Ontario a décidé qu'il ne devrait pas y avoir de vote en réseau le jour du scrutin.

LE VOTE EN RÉSEAU COMME COMPLÉMENT DU VOTE SUR PAPIER

En outre, le directeur général des élections établit clairement que les modes de scrutin en réseau doivent être mis en œuvre à titre de complément du mode de scrutin sur papier et que le mécanisme actuel doit être disponible en tout temps au cours de l'événement. Les votants devraient être en mesure de s'inscrire au vote en réseau, puis de décider de voter sur papier, et vice- versa.

ATTÉNUER LE CHANGEMENT ORGANISATIONNEL

Élections Ontario a également décidé que comme la mise en œuvre du projet pilote ne mènera peut-être pas nécessairement à la mise en œuvre de la même solution pour une élection générale, les changements imposés à l'organisation devraient être minimaux. L'approche envisagée dans le cadre du projet pilote devrait par conséquent être conçue de manière à produire le moins d'impact possible sur les gens, les processus et les systèmes d'élections Ontario. L'approche retenue devrait réduire au maximum les besoins d'intégration avec les systèmes et processus électoraux existants, en tenant compte, en particulier, des points d'intégration ayant trait à la liste des votants et à la communication des résultats.

Contraintes liées à l'échéancier

LE SYSTÈME DEVANT ÊTRE MIS À L'ESSAI DEVRAIT ÊTRE PRÊT D'ICI LE PREMIER TRIMESTRE DE 2012

Si l'on considère qu'un projet pilote fait partie du processus d'évaluation, le système de vote en réseau doit être prêt en vue d'une élection partielle en 2012 afin que la date de présentation d'un rapport du 30 juin 2013 soit respectée.

Contraintes de coûts

Compte tenu du fait que ce sont essentiellement les coûts liés aux produits et services du fournisseur qui détermineront les coûts réels du projet pilote sur le vote en réseau, aucune limite de coûts précise ne restreint les solutions recommandées dans le cadre du projet pilote.

LA SOLUTION DEVRAIT ÊTRE ÉCONOMIQUE

Toutefois, il existe une contrainte : l'approche de mise en œuvre devrait être la plus économique possible. Le document antérieur intitulé *Network Voting Options Research* a attribué une cote à chaque scénario sur la base d'une échelle relative d'économie.

Contraintes techniques

DES DONNÉES DEVRONT ÉTAYER LA MISE EN ŒUVRE DU VOTE EN RÉSEAU

Pour bien appliquer une solution de vote en réseau, il faut disposer de données et de renseignements clés afin d'appuyer le processus de vote. L'information figure sous différentes formes dans les systèmes d'information d'ÉO ou d'autres organismes provinciaux et il faudra y accéder dans le contexte de la solution de vote en réseau.

Deux composantes clés apporteraient des contributions essentielles à la mise en œuvre réussie du vote en réseau :

- une liste électorale en temps réel*;
- une méthode sûre d'établissement de l'identité des votants.

La liste électorale électronique existante (SGLE/SGE) doit être actualisée et refléter les modifications à la liste électorale en tout temps au cours d'un scrutin.

*sans liste en temps réel, chaque mode de scrutin devrait être verrouillé et géré séparément.

D'autres organismes provinciaux devraient se procurer les données d'authentification du votant qui ne sont pas présentement détenues par ÉO. L'organisme le plus susceptible d'accomplir cette tâche serait le service ONe-key[3], qui a été lancé par ServiceOntario, et qui est « conçu dans le but d'offrir un point d'accès commun aux programmes ontariens »; toutefois, l'intégration à ce service ne pourra être réalisée dans l'échéancier établi pour le projet pilote. Il faudra donc trouver d'autres moyens de bien authentifier les votants.

Sommaire des contraintes

Le tableau qui suit expose la liste complète des contraintes.

CATÉGORIE	CONTRAINTE
Liée à l'échéancier	Le projet pilote d'Élections Ontario doit être prêt d'ici janvier 2012.
Législative	La loi interdit le vote en réseau, mais les articles 4.1 et 44.3 combinés annulent cette interdiction dans le cas des élections partielles. L'article 44.2, qui entre en vigueur en janvier 2012, a le même effet pour les élections générales dans certaines circonstances[4].
Législative	Les données électorales, notamment les données saisies et archivées par un système de vote en réseau, doivent être archivées et déclassées pour une durée déterminée (recueillies pour l'ADP pendant l'inscription et les résultats de l'élection).
Liée au processus	Si possible, l'évaluation du vote en réseau devrait être effectuée dans le cadre d'un projet pilote au cours d'une élection officielle (vraisemblablement une élection partielle) et non en contexte de laboratoire / d'essai / de validation.
Liée au processus	Aucun vote en réseau le jour de scrutin.
Liée au processus	Les bulletins de vote sur papier doivent être disponibles en tout temps (ne pas retirer le mécanisme actuel – seulement y ajouter).
Liée au processus	La liste électorale électronique actuelle (SGLE/SGE) doit constamment être actualisée au cours d'un scrutin.
Liée au processus	Atténuer le changement organisationnel en définissant une approche ayant une incidence minimale sur les gens, les processus et les systèmes d'Élections Ontario.
Technique	Compte tenu du fait que l'accès à la bande passante n'est pas universel en Ontario, la solution ne devrait pas reposer sur la connectivité à haute vitesse, mais devrait s'efforcer raisonnablement de soutenir l'accès utilisable par un accès par réseau commuté sur le plan du temps de réponse à une transaction dans le système.
Technique	Les plans de recourir à information Technology Services (ITS) comme hôte de l'application pourraient introduire des contraintes additionnelles importantes, selon la longueur du cycle requis pour obtenir et parachever les ententes d'hébergement.
Technique	Seules les données suivantes sont archivées pour chaque électeur : code de circonscription électorale, nom de famille, prénom, second prénom, date de naissance, sexe, adresse municipale, adresse postale.
Technique	Les interfaces accessibles qui sont utilisées dans le projet pilote doivent correspondre au degré d'accessibilité fourni par les dispositifs accessibles de marquage des bulletins de vote existants d'ÉO.
Technique	Conserver le degré d'intégration et de changements aux systèmes existants à un niveau minimal pour le projet pilote.

2.3 PUBLIC CIBLE

En situation de projet pilote, une solution de vote en réseau s'adresserait à tout l'électorat plutôt qu'à un groupe ou à une population démographique en particulier au sein de l'électorat. Il en résulterait une base potentielle moyenne de votants d'environ 80 000 électeurs pour une élection partielle dans une seule circonscription électorale, les plus grandes circonscriptions électorales pouvant compter jusqu'à 130 000 électeurs.

SONDAGE POST-ÉLECTION DE 2007

L'électorat de l'Ontario est bien positionné pour l'instauration du vote en réseau. La recherche qui a trait au scrutin portant sur des élections récentes indique qu'une vaste proportion de la population est favorable au vote par internet[5], qui devient fréquent à l'échelon municipal. En outre, comme les ontariens affichent un taux élevé d'accès à internet et à l'infrastructure téléphonique et un taux élevé de connaissance de l'utilisation d'internet, l'Ontario est bien positionnée pour le vote en réseau.

Attitudes à l'égard du vote par internet

D'après le *sondage auprès des électeurs à la suite de la 40e élection générale* d'élections canada, 42 % des répondants de l'électorat ontarien seraient « très susceptibles » de voter par internet, ce qui représentait le taux le plus élevé parmi les provinces canadiennes.

Toutefois, le public et les médias perçoivent encore négativement le vote en réseau, au même titre qu'il existe des groupes opposés au concept de vote en réseau ou de vote électronique. Bien qu'il soit reconnu que ce n'est peut-être pas la perception dominante, la mise en œuvre devrait prendre en compte les réserves et les objections soulevées à l'encontre du vote en réseau.

Expérience du vote en réseau municipal

Plusieurs municipalités de l'Ontario ont utilisé la technologie de vote en réseau dans des élections officielles. Les exemples les plus récents comprennent Markham, Peterborough et Stratford, qui ont eu recours au vote en réseau lors des élections municipales de 2010 et ont partagé leurs expériences avec Élections Ontario au sommet d'apprentissage sur le vote électronique aux élections municipales de décembre 2010.

Afin de pouvoir voter aux élections de Peterborough ou de Markham, les votants ont généralement reçu une lettre par courrier, puis se sont inscrits par internet afin d'obtenir la qualité d'électeur définitive, qui a été attribuée par courriel à Peterborough et dans une deuxième lettre envoyée par la poste à Markham. Les votants de Stratford n'avaient pas besoin de s'inscrire à l'avance. Les votants ont pu exprimer leurs suffrages à distance dans les trois villes, Stratford offrant également la possibilité de se rendre dans des bureaux de scrutin. Des modes de scrutin en réseau ont été offerts en complément des bulletins de vote sur papier, sauf à Stratford où le vote par internet et par téléphone a remplacé les bulletins de vote sur papier.

Accès à internet

En 2009, 80 % des Canadiens âgés de 16 ans ou plus, soit 21,7 millions de personnes, se sont servis d'internet à des fins personnelles. Le taux d'accès est légèrement plus élevé en Ontario, où il s'établit à 81 % de la population[6]. Parmi ces utilisateurs d'internet, 75 % y ont recours au moins une fois par jour[7] et 66,7 % s'en servent à des fins bancaires ou pour acquitter des factures[8].

Toutefois, malgré ce taux d'accès élevé, il subsiste des réserves importantes au sujet de la sécurité et de la protection de la vie privée. Parmi les personnes qui ont dit se servir d'internet depuis moins de cinq ans, 55 % exprimaient de très sérieuses réserves au sujet de l'utilisation de cartes de crédit sur internet et 50 % au sujet des transactions bancaires réalisées sur internet. Ces proportions ont chuté à 42 % et 37 %, respectivement, dans le cas des personnes qui disent utiliser internet depuis cinq ans ou plus[9].

De plus, il semble exister une division entre les régions urbaines et les régions rurales quant à l'utilisation d'internet. En 2005, seulement 58 % des résidents vivant dans des régions rurales et dans de petites villes avaient accès à internet, soit beaucoup moins que la proportion constatée à l'échelle nationale. Cet écart entre les régions rurales et les régions urbaines pourrait refléter l'interaction d'autres facteurs socio-économiques ou illustrer d'autres effets, comme la disponibilité de la bande passante. L'accès à la bande passante, en particulier dans les régions rurales, n'est pas encore universel. Par conséquent, la solution retenue devrait être conçue pour bien fonctionner à des vitesses d'accès par ligne commutée plus lentes.

Accès au téléphone

L'enquête sur le service téléphonique résidentiel de 2006 a révélé que 92,5 % des ontariens ont une ligne à RTCP dans leur résidence. Parmi les foyers qui n'ont pas de ligne téléphonique (7,5 % des ontariens), 78,2 % disent bénéficier d'un service de téléphonie cellulaire et 31,7 % déclarent utiliser des services de téléphonie par câble ou des services « VoIP »[10]. L'enquête révélait également que 1,2 % des ménages n'avaient pas de service téléphonique du tout. Ce taux est demeuré inchangé par rapport à l'année précédente.

Utilisation de la technologie d'aide web

Les utilisateurs qui ont un handicap visuel peuvent se servir de lecteurs d'écran pour avoir accès à des pages web. Ces dispositifs d'aide interprètent le code HTML de la page et le reproduisent sous forme de discours. Bien que la conformité aux normes et pratiques d'accessibilité soit essentielle, toute solution de vote en réseau doit également être conçue expressément en gardant à l'esprit la compatibilité avec un lecteur d'écran. Se reporter à l'appendice c pour un exposé sur les lecteurs d'écran dans le contexte de l'accessibilité générale au web.

Une enquête menée en 2011 par WebAIM (un partenariat du Center for Persons with Disabilities et de la Utah State University) a conclu que 59 % des répondants utilisent JAWS comme lecteur d'écran principal, suivi de Windows-Eyes, d'Apple's VoiceOver, et de NVDA, tous dans une proportion d'environ 10 %[11].

Bien que JAWS et Windows-Eyes dominent toujours le marché, la comparaison des résultats avec ceux des enquêtes précédentes de WebAIM révèle que ces produits établis sont en baisse de popularité. Comme le montre la figure 2, à droite, JAWS et Windows-Eyes sont passés d'une utilisation par 97 % des usagers en 2009 à 70 % en 2011. Cette perte de part de marché résulte de la popularité croissante de nouveaux produits moins chers ou gratuits comme NVDA et VoiceOver, d'Apple.

Comme l'indiquent les conclusions de l'enquête, il n'y a « pas d'utilisateur type de lecteur d'écran ». Le système de vote en réseau devrait être conçu de manière à être compatible à la fois avec les produits principaux et avec une gamme raisonnable de produits qui comprennent des solutions de rechange gratuites et à faible coût. La compatibilité avec un logiciel à faible coût contribuera également à abattre les obstacles pour les utilisateurs qui ne se servent généralement pas de technologies d'aide web, mais qui pourraient être incités à le faire pour voter par internet.

Figure 4 : Part du marché en 2011

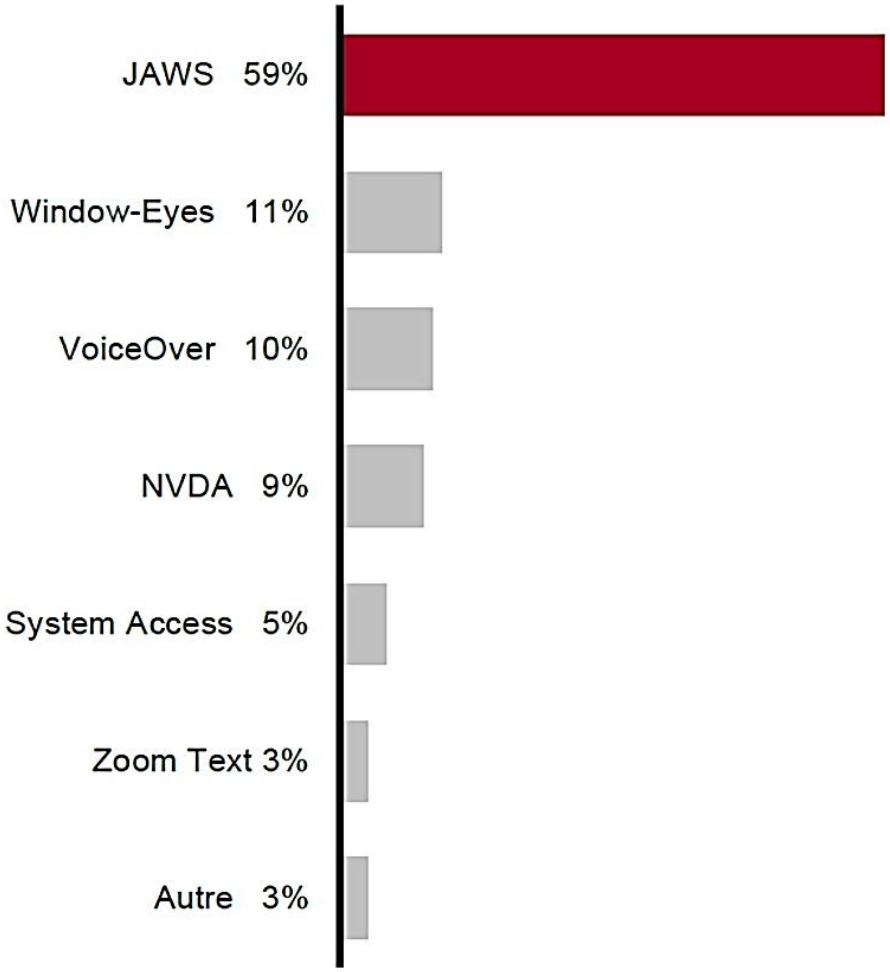
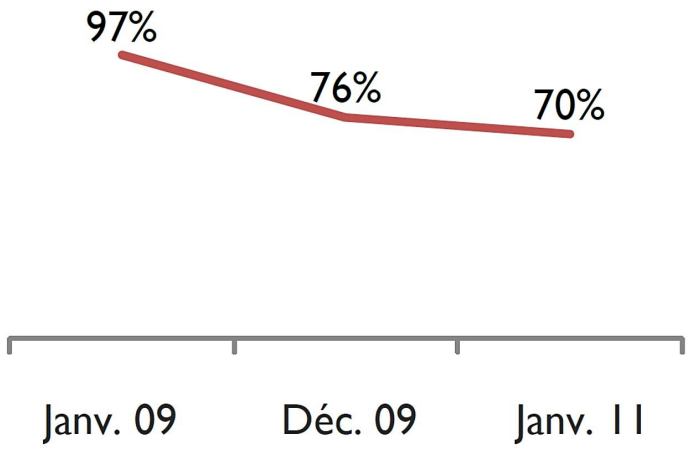


Figure 5 : JAWS et Windows-Eyes sont en perte de popularité



2.4 CONSULTATION AVEC LES PARTIES PRENANTES

COMITÉ CONSULTATIF SUR L'ACCESSIBILITÉ

La consultation à cette étape de l'initiative a été limitée à une consultation avec le comité consultatif sur l'accessibilité relevant du directeur général des élections. La présente section donne un aperçu de la méthodologie de consultation des membres du comité consultatif sur l'accessibilité (CCA). La consultation prenait la forme d'une série de questions conçues pour recueillir de l'information sur :

- les tendances et préférences en matière de scrutin;
- l'engagement technologique.

Processus et résultats

QUESTIONS ET RÉTROACTION

À la suite d'une séance d'information sur un projet tenue lors d'une réunion du CCA à Toronto le 26 janvier, un certain nombre de questions ont été présentées aux membres du comité qui ont répondu à celles-ci en table ronde. Des questions de suivi ont également été distribuées par courriel et les réponses ont été recueillies et analysées. La présente section résume les résultats de la rétroaction reçue. Prière de consulter l'Appendice b pour prendre connaissance d'une liste détaillée des questions.

AVANTAGES ET INCONVÉNIENTS

En ce qui concerne les avantages et les inconvénients du scrutin par internet, les membres du CCA ont relevé les avantages de l'accessibilité et le potentiel d'appuyer la dignité, l'indépendance et l'égalité d'accès pour tous les votants. Ils ont également mentionné l'existence d'un obstacle potentiel pour les électeurs n'ayant pas d'accès (ou de moyens d'accéder) à un ordinateur et à internet haute vitesse. L'absence d'aspect social du vote et la possibilité de méfiance de la part du public suscitent également des réserves.

Les membres du CCA ont fait observer que le vote par téléphone présentait l'avantage d'être plus facilement accessible, mais l'inconvénient de poser des problèmes d'accessibilité et de convivialité distincts. Ils ont également mentionné que bien qu'ils étaient plus utiles pour certains votants, les téléphones intelligents ne sont pas universellement accessibles.

CONFIANCE ET SÉCURITÉ

Pour ce qui est de l'importance relative des caractéristiques du vote en réseau, les membres du CCA classaient presque à l'unanimité la C*onfiance dans le système* et la S*écurité* comme les deux caractéristiques principales du vote en réseau. En outre, l'accent était largement mis sur la protection de la vie privée, et sur la commodité et la facilité d'utilisation.

L'accent était mis presque à l'unanimité sur le potentiel du CCA de prendre part à des essais d'acceptation par l'utilisateur (EAU) pour le vote en réseau. Que ce soit à titre de participants aux essais eux-mêmes ou en aidant à superviser le choix des personnes devant participer aux essais, ce thème s'est révélé très fort dans l'ensemble des réponses. Ils estimaient que l'ampleur de leurs compétences positionnait bien les membres du CCA pour contribuer au processus d'eau d'élections Ontario.

CONCEPTION UNIVERSELLE

Bon nombre des commentaires formulés au cours de la réunion du comité et d'une séance de suivi avec le conseiller en matière d'accessibilité d'Élections Ontario appuient vigoureusement la conclusion selon laquelle la technologie et le processus doivent être conviviaux et les plus universellement accessibles pour tous les électeurs – en mettant l'accent sur l'accommodement raisonnable et en évitant tout type de différence de traitement.

2.5 HYPOTHÈSES DE TRAVAIL

Pour élaborer la liste de recommandations la plus exacte et la plus complète possible, certaines conditions doivent être évaluées, qui ne peuvent être connues d'avance ou ne peuvent être décrites adéquatement par des principes ou des contraintes. Ces hypothèses comprennent les caractéristiques d'une élection partielle possible et des hypothèses opérationnelles générales.

Caractéristiques de l'élection partielle

Sur la base d'une analyse d'élections partielles tenues en Ontario au cours des cinq dernières années, il ressort que plusieurs caractéristiques ont des répercussions sur la planification et la taille d'un projet pilote de vote en réseau.

Figure 6 : Statistiques choisies d'une élection partielle

		Inscriptions et révisions	Participation	Bureaux de vote par anticipation	Total des votes déposés	Votes déposés dans les bur. de vote par anticipation	Votes déposés dans les bur. de vote par anticipation	Votants inscrits qui ont utilisé les bur. de vote par
2010	Ottawa West-Nepean	86,809	33%	4	28,595	2,267	8%	3%
	Leeds-Grenville	76,053	37%	10	27,846	3,709	13%	5%
	Toronto Centre	96,846	33%	4	26,177	2,033	8%	2%
2009	St. Paul's	83,183	33%	5	27,830	3,353	12%	4%
	Haliburton-Kawartha	90,351	39%	10	35,541	6,370	18%	7%
2007	Burlington	77,749	29%	11	22,834	2,733	12%	4%
	York South-Weston	66,308	29%	6	18,977	1,328	7%	2%
	Markham	110,902	17%	14	18,522	1,901	10%	2%
	Toronto-Danforth	68,782	40%	5	27,437	3,129	11%	5%
2006	Nepean-Carleton	105,802	29%	8	30,170	3,251	11%	3%
	Parkdale-High Park	73,317	39%	14	28,646	2,226	8%	3%
	Whitby-Ajax	106,028	32%	5	34,376	4,623	13%	4%

Statistiques choisies d'une élection partielle 2006-2010

Valeurs maximales des indicateurs clés en rouge.

Tel qu'il est indiqué dans le tableau qui précède, de huit à treize pour cent des votes à l'élection partielle peuvent être exprimés lors du vote par anticipation (dans le cas des élections partielles, le scrutin par anticipation s'étend sur six jours au cours de la période de sept jours qui se termine le sixième jour avant le jour de scrutin. voir le paragraphe 44(3) de la loi électorale.) qui s'étend sur six jours, le nombre de bureaux de vote allant de cinq à quatorze. Si Markham, qui peut compter jusqu'à 110 000 électeurs (nombre confirmé : 133 000) a vécu un taux de participation plus près du taux de participation moyen à l'élection partielle de trente-deux pour cent et du taux moyen de vote par anticipation de onze pour cent, cela se traduirait par près de 5 000 voix exprimées dans quatorze bureaux.

Si le vote en réseau suscite le même intérêt qu'au cours des élections municipales tenues récemment, près de 10 000 votes pourraient être exprimés au moyen des modes de scrutin en réseau. De fait, quatre-vingt-dix pour cent des votants de Markham ont indiqué au cours d'une enquête tenue en 2010 qu'ils voteraient par internet à l'échelle provinciale ou fédérale s'ils le pouvaient[12].

On peut raisonnablement s'attendre à ce que la publicité qui entoure l'introduction du vote en réseau dans une élection partielle provinciale ait deux effets pertinents : que les modalités du vote évoluent vers l'utilisation du vote par anticipation, et que ce changement amène l'adoption de modes de scrutin en réseau à un rythme similaire à celui qui a été observé lors de récentes élections municipales (de 10 % à 20 % des suffrages[13]). à des fins pratiques, la solution recommandée devrait par conséquent pouvoir fonctionner simultanément dans quatorze bureaux de vote par anticipation et, à tout le moins, répondre aux besoins de dix mille électeurs qui accèdent au système pendant six journées de dix heures.

Le système devrait prendre en charge 10 000 votes sur une période de vote par anticipation de six jours.

3. PRINCIPES : ÉVALUATION DU VOTE EN RÉSEAU

Pour toute initiative de cette importance, il faut utiliser un ensemble de données bien définies afin d'évaluer le succès. Le présent chapitre donne un aperçu de la méthodologie utilisée pour élaborer une liste de principes de base qui sont employés pour évaluer les scénarios de vote en réseau dans cette étude de cas et qui finiront par être utilisés pour mesurer le succès de la solution du vote en réseau et pour établir qu'un projet pilote pourrait peut-être être considéré.

CHOISIR LES PRINCIPES DE BASE

Afin de créer une étude de cas valide sur le vote en réseau, il doit y avoir un lien direct entre les critères utilisés pour évaluer les options de vote en réseau, l'étude de cas sur les options privilégiées, et la réussite de la solution éventuelle sur le vote en réseau et (ou) du projet pilote. Le fondement de ces critères doit pouvoir être relié à un ensemble de base de principes de vote.

3.1 PRINCIPES ÉLECTORAUX

Toute élection doit être universelle, égale, libre et secrète; de plus, tout système de vote en réseau doit satisfaire à l'exigence de base qui consiste à étayer ces principes fondamentaux. Il convient de définir une liste complète des principes avant de définir le sous-ensemble des principes de base qui orienteront l'analyse, les recommandations et la mise en œuvre d'un vote en réseau. Aux fins de cette analyse, ces principes sont répartis en deux groupes* :

- **Les principes universels**, qui sont tirés des quatre principes fondamentaux que sont l'universalité, l'égalité, la liberté et le secret.
- **Les principes procéduraux**, tirés de trois mécanismes procéduraux fondamentaux qui sont nécessaires pour étayer les principes universels : transparence, vérifiabilité et responsabilisation, et fiabilité et sécurité.

*les principes utilisés aux fins de cette analyse reposaient sur ceux qui étaient recommandés par le conseil de l'Europe.

PRINCIPES UNIVERSELS

Le tableau qui suit illustre les principes détaillés issus des quatre principes universels de base[14] :

1. Universalité
    1.1. Facilité d'emploi
    1.2. Accessibilité
    1.3. Facilité d'atteinte (emplacement)
2. Égalité
    2.1. Un votant, un vote
    2.2. Pas de votants privilégiés
    2.3. Pas d'acteurs privilégiés
    2.4. Authentification et autorisation du votant
    2.5. Droit de figurer sur la liste des votants
    2.6. Prise en compte des suffrages exprimés par des votants admissibles uniquement
    2.7. Organisation juste du bulletin de vote
    2.8. Absence de coût pour les votants
    2.9. Production d'une liste des votants juste
3. Liberté
    3.1. Ni contrainte ni vente de votes
    3.2. Vérifiabilité au cas par cas
    3.3. Intégrité
4. Secret
    4.1. Confidentialité des données personnelles
    4.2. Secret du bulletin de vote
    4.3. Confidentialité
    4.4. Pas de résultats intermédiaires
    4.5. Déclassement des données protégées

PRINCIPES PROCÉDURAUX

Le tableau qui suit illustre les règles de procédure ou lignes directrices détaillées tirées des trois principes procéduraux fondamentaux :

1. Transparence
    1.1. Formation du votant
    1.2. Information/diffusion
    1.3. Facile à expliquer aux votants
2. Vérifiabilité et responsabilisation
    2.1. Vérifiabilité du code source
    2.2. Vérifiabilité du processus
    2.3. Certification
    2.4. Validation des résultats
    2.5. Surveillance de l'élection
    2.6. Examen des fichiers journaux/investigation
    2.7. Reprises partielles possibles
3. Fiabilité et sécurité
    3.1. Disponibilité du service
    3.2. Pas de point de confiance commun
    3.3. Intégrité de la plateforme
    3.4. Contrôle d'accès
    3.5. Intégrité de l'urne
    3.6. Intégrité des fichiers journaux
    3.7. Intégrité de la liste des votants
    3.8. Intégrité de la configuration de l'élection
    3.9. Intégrité des bulletins de vote

3.2 ÉVALUATION DES PRIORITÉS

Afin de définir l'ensemble de base des principes de vote en réseau, chaque élément de la liste complète des principes universels et procéduraux (voir ci-haut) s'est vu attribuer l'un des trois niveaux de priorité (élevé, moyen, et faible). Les principes ayant obtenu le niveau de priorité le plus élevé sont ceux avec lesquels le succès du projet pilote sera mesuré.

RANG PRIORITAIRE

Élevé – Ces principes seront utilisés pour mesurer le succès du projet pilote dans une élection partielle et pour évaluer s'il convient d'appliquer le vote en réseau à une élection provinciale. Ces renseignements seront utilisés comme critères dans les options de vote en réseau et dans les documents sur l'étude de cas.

Moyen – Ces principes constitueront le système obligatoire et les exigences procédurales de l'étude de cas (et du système qui fait l'objet du projet pilote). Ils seront définis à titre d'exigences des options de vote en réseau et des documents de l'étude de cas ainsi que dans la DDP en vue de l'obtention d'une solution en réseau.

Faible – Ces principes seront utilisés à titre de système souhaitable et d'exigences procédurales de l'étude de cas (et du système qui fait l'objet du projet pilote). Ils seront utilisés comme critères dans les options de vote en réseau ainsi que dans la DDP en vue de l'obtention d'une solution en réseau.

MÉTHODOLOGIE

La méthodologie ayant été appliquée pour établir les catégories tenait compte des réponses aux questions suivantes sur le projet pilote sur l'élection partielle :

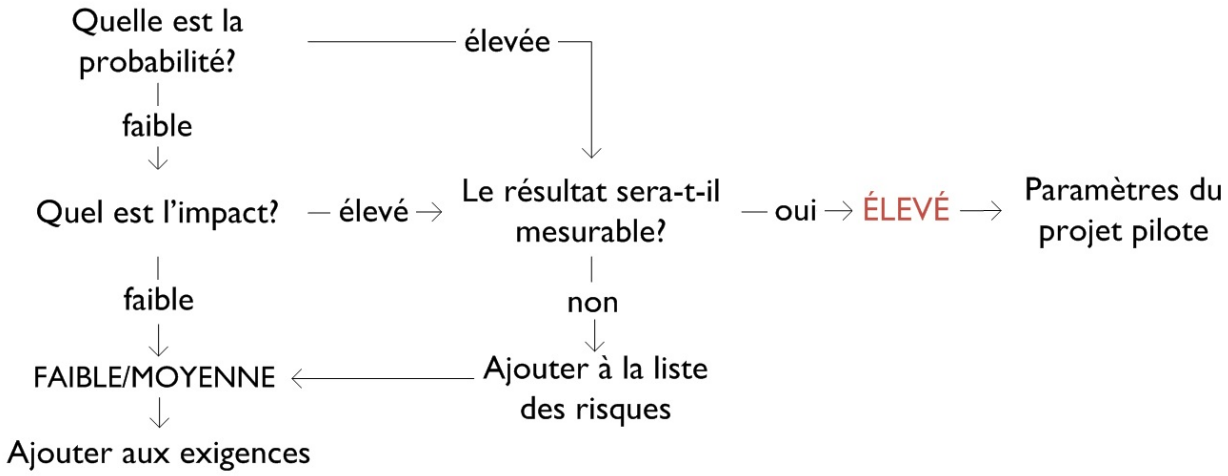
Le résultat sera-t-il difficile à mesurer ou à vérifier?

Quelle est la probabilité que la capacité de respecter le principe soit contestée en contexte de vote en réseau?

Quel serait l'impact d'un défaut éventuel de respecter le principe? En d'autres termes, le défaut aurait-il une incidence sur la perception à l'égard du vote en réseau aux échelons provincial et fédéral?

Les principes ont été classés de priorité élevée si *soit* a) ils présentaient une probabilité élevée d'être contestés *soit* b) ils présentaient une incidence d'échec élevée *et* c) que le résultat peut être mesuré de manière quantifiable. Le diagramme qui suit illustre la logique utilisée pour déterminer les principes à priorité élevée.

LOGIQUE DE SÉLECTION



3.3 LISTE BRÈVE DES PRINCIPES

La courte liste de principes qui suit a été élaborée au moyen de la méthodologie décrite précédemment. Les chiffres adjacents à chaque principe renvoient à la numérotation utilisée dans la liste complète des principes donnée dans la section suivante. Ces principes serviront à mesurer le succès du projet pilote lors d'une élection partielle et à évaluer si le vote en réseau doit être appliqué à une élection provinciale. Ces renseignements seront utilisés comme critères dans les options de vote en réseau et dans les documents sur l'étude de cas.

PRINCIPE	CRITÈRES	JUSTIFICATION
Accessibilité[1.2]	**coché** Mesurable **coché** Probabilité élevée **coché** Incidence élevée	Offrir à tous les ontariens des possibilités de voter intégrées et égales qui respectent l'indépendance et la confidentialité de chaque électeur est l'un des moteurs clés de l'initiative de vote en réseau et donne une visibilité élevée auprès du public.
Un votant, un vote[2.1]	**coché** Mesurable probabilité élevée **coché** incidence élevée	Une solution de vote électronique introduit des éléments de vulnérabilité apparents sur le plan de la sécurité qui n'existent pas dans le cas du bulletin de vote sur papier. Si le dépouillement des votes est compromis, la perception qu'a le public d'Élections Ontario serait mise en péril et l'intégrité des résultats de l'élection serait affectée.

PRINCIPE	CRITÈRES	JUSTIFICATION
Authentification et autorisation du votant[2.4]	**coché** Mesurable **coché** probabilité élevée **coché** incidence élevée	Un mode de vote en réseau doit offrir une façon réalisable d'authentifier l'identité du votant à distance. Cette situation pose des difficultés; aucune infrastructure provinciale n'existe pour authentifier numériquement les votants. Bien que serviceOntario soit l'organisme logiquement retenu, il faudra du temps et des efforts pour mettre en œuvre un protocole de validation de transfert avec la liste d'électeurs d'ÉO et l'ensemble actuel des services de serviceOntario.
Prise en compte des suffrages exprimés par des votants admissibles seulement[2.6]	**coché** Mesurable Probabilité élevée **coché** Incidence élevée	si des suffrages autres que ceux exprimés par des votants valides et admissibles avaient été dénombrés, l'intégrité de l'élection serait gravement affectée. un système de vote en réseau peut être vulnérable à une ingérence malicieuse ou au remplissage de bulletins de vote d'une façon non permise par le système de bulletins de vote sur papier. Le vote par internet pourrait attirer les pirates et l'incidence mettrait en péril les résultats de l'élection.
Vérifiabilité au cas par cas[3.2]	**coché** Mesurable **coché** Probabilité élevée **coché** Incidence élevée	Il pourrait être difficile de fournir aux votants le même sentiment de vérification que celui que donne le système du bulletin de vote sur papier / de l'urne. Le défaut de donner au votant de la rétroaction pour vérifier que son vote a été inscrit peut remettre en question les résultats et ÉO et nuire à la perception du vote en réseau.
Confidentialité[4.3]	**coché** Mesurable Probabilité élevée **coché** Incidence élevée	La probabilité qu'un système de vote en réseau compromette les données du votant et les résultats est faible, mais si cela se produit, l'impact compromettrait la confiance du public envers ÉO.
Validation des résultats[6.4]	**coché** Mesurable Probabilité élevée **coché** Incidence élevée	La validation des résultats est un principe fondamental des élections et la capacité d'étayer un recomptage ou une vérification est cruciale. Le défaut de le faire remettrait en question les résultats de l'élection et aurait un impact sur les solutions futures de vote en réseau.
Disponibilité du service[7.1]	**coché** Mesurable Probabilité élevée **coché** Incidence élevée	Bien que la perception qu'a le public de l'arrêt du système puisse être atténuée, il se peut que l'électorat ne pardonne pas aussi facilement une interruption provinciale. Les pannes de système seront rapportées dans les médias et auraient un impact sur la perception qu'a le public des solutions de vote en réseau.

4. QU'EST-CE QUE LE VOTE EN RÉSEAU?

Le chapitre suivant donne un aperçu de certains concepts clés du vote en réseau, notamment des éléments et des acteurs principaux, ainsi que des méthodes utilisées pour déposer des votes et établir et vérifier l'identité du votant.

LE VOTE EN RÉSEAU EST UN MODE de scrutin et de dépouillement par voie électronique qui repose sur la transmission des bulletins de vote et des suffrages par téléphone, par réseau informatique privé ou par internet. La technologie du vote en réseau peut donner aux électeurs de l'Ontario des options autres que les bulletins de vote sur papier traditionnels en leur permettant d'exprimer des suffrages par internet, par borne interactive ou par téléphone.

Le présent chapitre donne un aperçu des éléments de base de la mise en œuvre générale du vote en réseau :

- les composantes d'un système de vote en réseau de base;
- les méthodes pouvant être utilisées pour voter;
- les mécanismes qui peuvent être utilisés pour établir l'identité d'un votant lorsqu'il vote.

4.1 UN SYSTÈME DE VOTE EN RÉSEAU DE BASE

Comme le montre le diagramme ci-après, un système de vote en réseau comprend des composantes technologiques, comme un réseau et un centre de données et des acteurs, comme des votants et du personnel électoral, qui interagissent avec ces composantes.

Votant : Un votant est un électeur qui a accès à la plateforme de votation pour voter. Pour ce faire, un votant utilise un dispositif de votation, d'un bureau de vote ou à distance.

Membre du personnel de scrutin : Si le vote sur site est mis en œuvre, le responsable de l'élection doit avoir formé du personnel pour superviser le processus de vote électronique sur site et apporter son aide.

Centre d'appels : Tout scénario de vote en réseau requiert un centre d'appels pour appuyer les votants et les membres du personnel de scrutin.

Réseau : Le réseau est le mode ou les modes utilisés par les divers acteurs pour communiquer entre eux. Ce peut être internet, le réseau cellulaire, le réseau de service téléphonique à fil ou autres.

Centre de données : Ce centre accueille les plateformes de votation et stocke les bulletins de vote électroniques jusqu'à la fermeture des bureaux de scrutin et au traitement des bulletins par les autorités électorales. Un centre de données de sauvegarde peut être mis en place pour prendre le relais si le centre de données principal est défaillant.

Administrateur de système : Le personnel qui opère et tient le centre de données, y compris les serveurs et l'urne électronique.

Serveurs de l'élection : L'infrastructure technique requise pour accueillir et protéger le système de vote électronique.

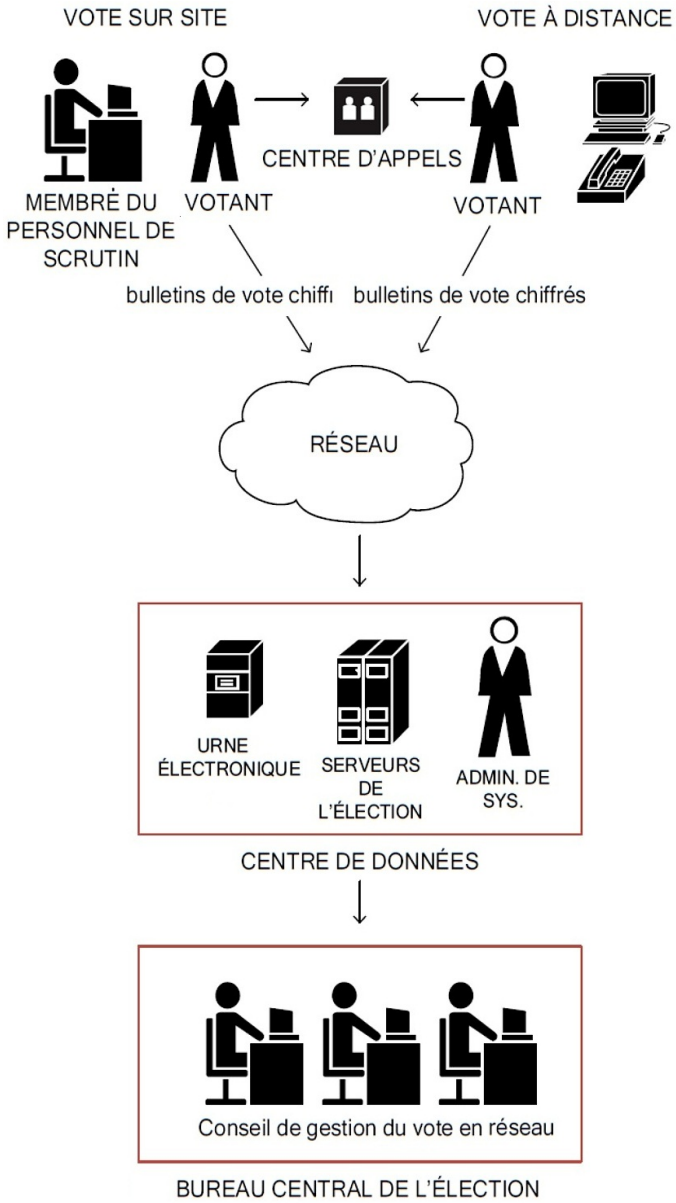
Urne électronique : Endroit (généralement une base de données) où les suffrages exprimés sont archivés en attendant le traitement final.

Bureau central de l'élection : Endroit où la définition de l'élection a lieu. Lorsque les bureaux de scrutin ferment, les bulletins de vote électroniques sont traités ici (et groupés avec les résultats des autres modes de scrutin) par le conseil de gestion du vote en réseau.

Conseil de gestion du vote en réseau : Le groupe des personnes chargées de superviser le traitement des bulletins de vote électroniques.

Éléments optionnels (non illustré) : Selon le mécanisme de vote, des éléments peuvent être présents dans le scénario, comme un système RVI ou une passerelle SMS.

Figure 7 – Composantes et acteurs clé



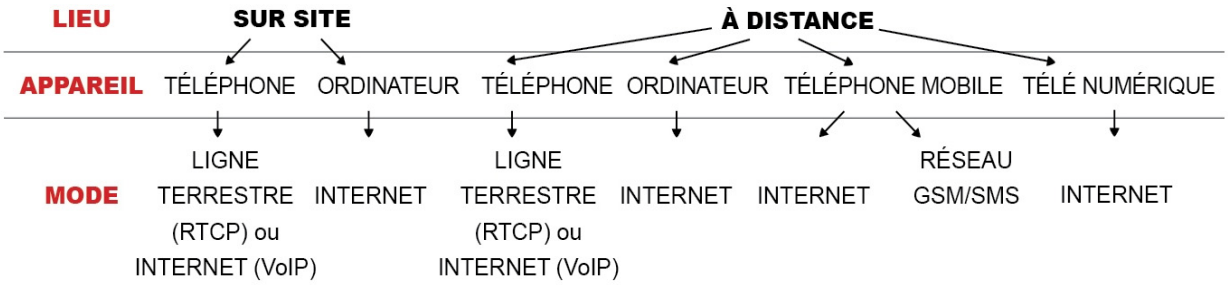
Certains éléments doivent être en place pour appuyer un tel système :

- Le centre de données (où les serveurs de l'élection se trouvent et où les bulletins de vote sont traités) doit être fiable et sûr.
- Les responsables de l'élection doivent préparer toutes les données requises pour configurer le système de vote.
- De nouvelles procédures doivent être créées pour les nouvelles activités que le vote en réseau ajoute au mécanisme de vote avec bulletin en papier.
- Une certaine forme de mécanisme de vérification pour valider le système de vote.
- Une campagne de communications et de sensibilisation du public pour présenter les nouveaux mécanismes de vote à la population.

4.2 MODES DE SCRUTIN

Comme l'illustre le diagramme qui suit, les modes de scrutin peuvent être classifiés d'après le lieu où les suffrages sont exprimés, les dispositifs utilisés pour voter, et le mode utilisé pour transmettre les votes aux serveurs.

Figure 8 : Modes de scrutin



COMBINAISONS POSSIBLES

En combinant les lieux, les dispositifs et les modes figurant dans ce diagramme, il est possible de créer sept méthodes de base :

1. Vote sur site, par téléphone
2. Vote sur site, par ordinateur
3. Vote à distance, par téléphone
4. Vote à distance, par ordinateur, sur internet
5. Vote à distance, par téléphone mobile, sur internet
6. Vote à distance, par téléphone mobile, par SMS
7. Vote à distance, par télé numérique, sur internet

Même après une brève analyse, ce ne sont manifestement pas toutes ces combinaisons qui peuvent être utilisées en Ontario dans les conditions actuelles. Les infrastructures utilisées par la télé numérique et les SMS sont intrinsèquement moins sûres parce que des tiers (sociétés de câble, fournisseur de téléphonie cellulaire) deviennent des parties de confiance de la chaîne de vote. Bien que la télévision numérique soit très répandue, elle ne l'est pas suffisamment en Ontario pour qu'il vaille présentement la peine de l'utiliser comme base d'un mode de scrutin. Ce qui laisse des variantes du vote par internet (à partir d'un ordinateur ou d'un appareil mobile) et du vote par téléphone (à partir d'une ligne fixe ou d'un téléphone mobile) comme méthodes pouvant très bien être utilisées en Ontario.

4.3 MÉCANISME D'AUTHENTIFICATION

La méthode ou le mode de transmission du vote (internet, téléphone, etc.) n'est qu'une partie du portrait. Il est beaucoup plus difficile de créer un système qui peut établir l'identité du votant avec confiance. En termes techniques, le processus qui exige qu'un utilisateur de système prouve son identité est appelé *authentification*. L'authentification va de pair avec un autre processus – l'*autorisation* – qui, une fois l'identité vérifiée, détermine les gestes qu'un utilisateur peut poser.

Dans les systèmes de vote en réseau, les techniques d'authentification du votant peuvent être subdivisées en trois grandes catégories, selon celle qui est utilisée comme base de la sécurité de l'authentification.

1. **Information** – Le système demande quelque chose que seul le votant et l'authentification connaissent, comme un NAS ou un numéro de carte santé. Le votant ne doit pas révéler cette information à des tiers.
2. **Justificatifs d'identité** – Le votant a un justificatif d'identité qu'il est le seul à pouvoir posséder, sans être tenu de l'envoyer à l'authentificateur (le système de vote). Dans le cas de l'authentification électronique, cette méthode d'authentification repose souvent sur l'utilisation de cartes d'identité intelligentes protégées par un NIP. Il pourrait aussi s'agir d'une carte d'identité physique.
3. **Caractéristiques physiques** – L'authentificateur procède à la saisie des données biométriques du votant (comme les empreintes digitales) et vérifie qu'elles correspondent à celles qui sont archivées dans une base de données (p. ex., la liste électorale).

Comme dans l'aperçu précédent des modes de scrutin, il est clair que certaines de ces options d'authentification ne peuvent présentement être utilisées en Ontario. Aucune ID gouvernementale ne prend présentement en charge un certificat numérique qui pourrait être utilisé par un système de vote en réseau[15]. En outre, le gouvernement de l'Ontario et le gouvernement canadien ne stockent pas de données biométriques qui pourraient être utilisées à des fins d'authentification du votant. Il reste donc peu d'options viables. Les trois premières sont basées sur de l'information sous forme de mots de passe ou de renseignements personnels, et la dernière est fondée sur des justificatifs d'identité :

Utilisation d'un mot de passe. Chaque utilisateur reçoit un identificateur d'utilisateur ou un code d'utilisateur et un mot de passe qui leur est associé. Le code d'utilisateur correspond à l'identité de l'utilisateur, et le mot de passe est la preuve qui appuie ce nom. Le mot de passe est généralement une suite de caractères (lettres ou chiffres) utilisée pour prouver l'identité du votant et pour donner accès au système. Ce mot de passe tient lieu de secret partagé entre l'utilisateur et le système, qui vérifie alors l'admissibilité du votant à accéder au bulletin de vote.

Utilisation de données personnelles secrètes. L'entité responsable de l'élection doit avoir accès aux données personnelles de chaque votant que ce dernier saisit pour avoir accès au système. Les données elles-mêmes peuvent notamment comprendre, s'il y a lieu, le nom du votant, son adresse, sa date de naissance, son numéro d'identification, son numéro de téléphone cellulaire, son adresse courriel. Plus les données utilisées à des fins d'authentification deviennent secrètes, plus le degré de sécurité augmente. En raison de l'éventail limité des données personnelles stockées par Élections Ontario ou auxquelles Élections Ontario a accès pour chaque électeur, ce genre d'authentification *à lui seul* ne procurerait pas le degré de sécurité requis pour le vote en réseau en Ontario. Le recours aux données personnelles peut toutefois être utilisé de concert avec l'authentification du mot de passe pour contribuer à renforcer le niveau de confiance global.

Systèmes d'authentification tiers. L'authentification est déléguée à un système tiers comme un site Web gouvernemental ou un site bancaire en ligne. Le votant se connecte sur le site tiers, qui partage alors suffisamment de données relatives à l'identité avec le système de vote pour confirmer l'admissibilité du votant et donner accès au bulletin de vote électronique. Malheureusement, aucun système n'est présentement intégré aux systèmes d'Élections Ontario et la complexité d'une telle intégration serait trop grande à mettre en œuvre pour en faire un projet pilote[16].

Utilisation d'une ID physique (permis de conduire, passeport) pour prouver l'identité. Ce peut être fait seulement en personne dans un bureau de scrutin. Comme cette démarche prouve l'identité du votant seulement à un être humain et non au système lui-même, un autre mécanisme est nécessaire pour autoriser le votant à utiliser le système pour voter.

5. CONCLUSIONS DE RECHERCHE

Le chapitre précédent donnait un aperçu des composantes de base et du fonctionnement d'un système de vote en réseau. Il décrivait les méthodes pouvant être utilisées pour voter et les mécanismes qui peuvent être employés pour établir l'identité d'un électeur. Il donnait aussi un aperçu des modes de scrutin et des mécanismes d'authentification qui ne peuvent présentement être utilisés en Ontario. Le chapitre qui suit présente les conclusions d'une recherche détaillée sur les dix autres méthodes et mécanismes.

MATRICE DE RELATION

Les modes de scrutin et mécanismes d'authentification décrits dans les chapitres précédents peuvent se combiner pour créer une matrice des *scénarios* potentiels de vote en réseau. Le diagramme ci-après illustre l'ensemble des combinaisons possibles et recense les dix scénarios qui ont fait l'objet de la recherche :

Les combinaisons impossibles en environnement réel sont marquées **S.O.**

Les combinaisons dont la mise en œuvre n'est pas réalisable en Ontario sont marquées **NR** (non réalisables).

Les autres scénarios réalisables sont numérotés de **1** à **10**.

	ID physique	**Certificats numériques**	**Mots de passe**	**Données personnelles**	**Système tiers**	**Données biométriques**
Vote sur site, par ordinateur	**1**	NR	**3**	NR	**8**	NR
Vote sur site, par téléphone	**2**	S.O.	**4**	NR	S.O.	NR
Vote à distance, par téléphone	S.O.	S.O.	**5**	NR	S.O.	NR
Vote à distance par ordinateur, par internet	S.O.	NR	**6**	NR	**9**	NR
Vote à distance par téléphone mobile, par internet	S.O.	NR	**7**	NR	**10**	NR
Vote à distance par téléphone mobile, par SMS	S.O.	S.O.	NR	NR	NR	S.O.
Vote à distance par télé numérique, par internet	S.O.	S.O.	NR	NR	NR	S.O.

Les modes de scrutin basés sur les SMS ou la télé numérique, et les options d'authentification fondées sur les certificats numériques ou sur l'utilisation de données personnelles et biométriques ont été éliminés de la recherche détaillée parce qu'ils ne s'appliquent pas assez bien en Ontario. Ces technologies et approches étaient réputées trop risquées ou tout simplement non réalisables.

Chacun des dix scénarios a fait l'objet de recherches détaillées mettant l'accent sur leurs avantages, leurs inconvénients et leurs risques. Chaque scénario a ensuite été coté en regard des principes et des contraintes dont il est question dans les chapitres 2 et 3, qui précèdent :

1. Vote sur site, par ordinateur, avec authentification fondée sur une identification physique
2. Vote sur site, par téléphone, avec authentification fondée sur une identification physique
3. Vote sur site par ordinateur, par internet, avec authentification basée sur un mot de passe
4. Vote sur site par téléphone avec authentification basée sur un mot de passe
5. Vote à distance par téléphone avec authentification basée sur un mot de passe
6. Vote à distance par ordinateur, par internet, avec authentification basée sur un mot de passe
7. Vote à distance par téléphone mobile, par internet, avec authentification basée sur un mot de passe
8. Vote sur site par ordinateur, avec authentification basée sur les systèmes tiers existants
9. Vote à distance par ordinateur, par internet, avec authentification basée sur des tiers
10. Vote à distance par téléphone mobile, par internet, avec authentification basée sur des tiers.

MÉTHODE DE RECHERCHE

Dans le cadre de la recherche, un examen détaillé des documents sur le vote en réseau et des travaux de recherche sur la mise en œuvre récente du vote en réseau en Europe, au Royaume-Uni, en Australie et aux États-Unis ont été réalisés. Cette recherche a permis de documenter les avantages, les inconvénients et les risques propres à chacun des dix scénarios. De plus, chaque scénario a été évalué en regard des huit principes mesurables qui ont été définis dans le chapitre 3. Les résultats ont été documentés sous forme de cote relative. Prière de se reporter au document *Network Voting Options Research* pour obtenir tous les détails.

5.1 SCÉNARIO 1 : VOTE SUR SITE PAR ORDINATEUR, AVEC AUTHENTIFICATION FONDÉE SUR UNE IDENTIFICATION PHYSIQUE

VOTE SUR SITE PAR ORDINATEUR AVEC AUTHENTIFICATION FONDÉE SUR UNE IDENTIFICATION PHYSIQUE

Dans ce scénario, les suffrages sont exprimés sur le site au moyen d'une variante de l'ordinateur de bureau. Les votants se présentent au bureau de vote et montrent une preuve d'identité au membre du personnel de scrutin. Ce peut être tout document accepté par le responsable de l'élection; il s'agit généralement d'un document d'identification avec photo délivré par le gouvernement, comme un passeport ou un permis de conduire. Le membre du personnel de scrutin valide alors l'admissibilité du votant en vérifiant son identité dans un registre du scrutin. Si le votant est admissible, le membre du personnel de scrutin lui donne accès au dispositif de vote, qui est généralement une méthode d'autorisation approuvée, comme une carte à puce intelligente programmable. Ce scénario permet aux votants d'imprimer un accusé de réception de bulletin de vote sécurisé à titre de preuve matérielle du votant lorsqu'ils ont voté par voie électronique.

Si ce scénario doit être combiné à un mode de scrutin à distance (comme ceux que les scénarios 5, 6 et 7 décrivent), le bureau de vote devra avoir accès à une liste électorale centralisée en temps réel afin que les votants ne puissent voter plusieurs fois.

Avantages

- le vote sur site avec identification physique demeure le mécanisme le plus sûr pour identifier et autoriser les votants.
- degré de sécurité le plus élevé qui puisse être atteint : le responsable du scrutin contrôle les ordinateurs, et le réseautage peut être privé.
- permet à Élections Ontario de contrôler les environnements physique et informatique pour offrir un niveau élevé de facilité d'utilisation et d'accessibilité.

Inconvénients

- ajoute de la complexité pour les gens, les processus et les systèmes d'élections Ontario.
- nécessite un effort de logistique important pour préparer, déployer et déclasser l'équipement de vote en réseau.
- nécessite une formation spécialisée pour les membres du personnel de scrutin, le personnel de soutien, les équipes techniques, et ainsi de suite.
- les votants doivent quand même visiter un bureau de vote pour voter.

Risques

- dépend du courant et de l'infrastructure de réseautage/de la couverture qui existent dans chaque bureau de scrutin.
- dépend d'une liste électronique centrale des votants pour s'assurer de l'application de la règle « un votant, un vote ». Il existe des solutions de rechange à une liste centrale, mais elles limitent l'utilité de ce scénario si elles sont combinées au vote à distance.

5.2 SCÉNARIO 2 : VOTE SUR SITE PAR TÉLÉPHONE AVEC RTCP ET AUTHENTIFICATION FONDÉE SUR UNE IDENTIFICATION PHYSIQUE

VOTE SUR SITE PAR TÉLÉPHONE AVEC AUTHENTIFICATION FONDÉE SUR UNE IDENTIFICATION PHYSIQUE

Comme dans le scénario 1, les votants se présentent à un bureau de vote et montrent une preuve d'identité à un membre du personnel de scrutin, qui valide alors l'admissibilité du votant en comparant son identité au registre du scrutin. Si le votant est admissible, le membre du personnel de scrutin lui donne accès au dispositif de vote, soit, dans le présent cas, un téléphone.

Les téléphones utilisés pour exprimer des suffrages peuvent présenter plusieurs formats matériels (selon les technologies disponibles), et de nombreux modèles peuvent être combinés dans un seul bureau de vote. Les quatre systèmes téléphoniques de base qu'envisage ce scénario sont : RTCP standard, cellulaire standard, SIP et VOIP.

Comme les téléphones peuvent accepter uniquement des données numériques, l'autorisation est limitée à l'utilisation d'un numéro d'identification du votant (NIV) qui activera le bulletin de vote sonore. Cet identifiant unique peut être imprimé au préalable et présenté au votant dans une enveloppe scellée, ou le membre du personnel de scrutin peut choisir et attribuer un NIV au votant à partir d'une liste imprimée au préalable des numéros disponibles.

Le vote par téléphone ne peut donner d'accusé de réception du bulletin de vote déposé et par conséquent, ne peut offrir le même niveau de vérifiabilité qu'un ordinateur (au moyen d'une imprimante).

Si ce scénario doit être combiné à un mode de scrutin à distance (comme ceux que les scénarios 5, 6 et 7 décrivent), le bureau de vote devra avoir accès à une liste électorale centralisée en temps réel afin que les votants ne puissent voter plusieurs fois.

Avantages

- L'identification physique sur site constitue le mécanisme le plus sûr pour identifier et autoriser les votants.
- Il est possible de bien contrôler la sécurité, à l'exception d'une protection intégrale (voir les inconvénients).
- La facilité d'utilisation et l'accessibilité peuvent être très bonnes pour les votants ayant un handicap visuel.
- Le vote par téléphone est la façon la moins coûteuse (sur le plan de la logistique et des frais) d'offrir le vote en réseau dans les bureaux de vote; toutefois, quant au serveur, sa variabilité est bien moindre que dans le cas du vote par internet (le même serveur peut prendre en charge plus de votants par internet que de votants par téléphone).

Inconvénients

- Le vote sur site par téléphone nécessite un effort de logistique important pour préparer, déployer et déclasser l'équipement de vote en réseau, vérifier les lignes téléphoniques, la couverture du réseau cellulaire, et les réseaux (en particulier si le VOIP est utilisé).
- Nécessite une formation spécialisée pour les membres du personnel de scrutin, le personnel de soutien et les équipes techniques comptant des unités supplémentaires, et ainsi de suite.
- Les votants doivent quand même visiter un bureau de scrutin pour voter.
- Il est impossible d'obtenir une sécurité de bout en bout sans taxer considérablement la facilité d'utilisation : bien que les terminaux de votation soient contrôlés par le responsable de l'élection, les données qui quittent le téléphone ne sont pas protégées contre les attaques externes pouvant survenir dans le réseau (RTCP, cellulaire, etc.) ou par des attaques internes dans le système RVI.
- Non accessible pour les votants ayant un handicap auditif ou des handicaps moteurs graves.
- Le processus qui consiste à exprimer des suffrages est beaucoup plus long qu'au moyen d'un système informatique.

Risques

- Dépend de l'infrastructure téléphonique/de la couverture qui existent dans chaque bureau de vote et du courant et de l'infrastructure de réseautage en cas d'utilisation de VoIP.
- Possibilité d'attaques de type « intermédiaire » ou de mystification lors d'une séance de vote pendant que les données sont dans le RTCP.
- Dépend d'une liste électronique centrale des votants pour s'assurer de l'application de la règle « un votant, un vote ». Il existe des solutions de rechange à une liste centrale, mais elles limitent l'utilité de ce scénario si elles sont combinées au vote à distance.

5.3 SCÉNARIO 3 : VOTE SUR SITE PAR ORDINATEUR PAR INTERNET AVEC AUTHENTIFICATION BASÉE SUR UN MOT DE PASSE

VOTE SUR SITE PAR ORDINATEUR PAR INTERNET AVEC AUTHENTIFICATION BASÉE SUR UN MOT DE PASSE

Comme dans les scénarios 1 et 2, les votants se présentent à un bureau de vote pour exprimer leurs suffrages sur site; toutefois, dans ce scénario, les votants auront recours à une *authentification basée sur un mot de passe* plutôt qu'à une identification physique. Ce processus d'authentification basée sur un mot de passe permet aux votants de se rendre directement au terminal de votation sans montrer de preuve d'identité à un membre du personnel de scrutin. Le votant entre plutôt le justificatif d'identité lui-même au système de vote en saisissant un mot de passe unique distribué par l'intermédiaire du mode de livraison choisi par le responsable de l'élection. Ce scénario permet d'utiliser n'importe quel type de système de mot de passe (code d'utilisateur et mot de passe / NIV; usage traditionnel / unique), qui est saisi au moyen d'un périphérique ou d'un clavier à l'écran. Le système lui-même authentifie alors le votant et détermine son admissibilité à voter. Ce processus assure que chaque votant vote une seule fois.

Dans le cadre de l'authentification basée sur un mot de passe, le mode de livraison des mots de passe qui a été retenu doit présenter un équilibre entre la commodité et la sécurité, et des mesures de contrôle particulières doivent être fournies afin que chaque votant puisse obtenir seulement un mot de passe. Les modes de livraison peuvent comprendre la prise de possession sur site, le courrier physique, la distribution par voie électronique, un lien unique, ou la confirmation de données personnelles par un centre d'appels ou en ligne.

Une fois que le mot de passe est reçu, l'utilisation d'un clavier comme dispositif de saisie dans ce scénario peut occasionner des difficultés d'accessibilité pour certains utilisateurs; toutefois, il est généralement possible de surmonter ces difficultés au moyen de dispositifs d'aide à la saisie, ou en s'assurant le concours des membres du personnel de scrutin pour saisir le mot de passe au nom du votant. Ainsi, les membres du personnel de scrutin sont uniquement tenus de superviser le processus de scrutin et d'apporter de l'aide aux votants lorsqu'ils le demandent.

Comme dans le scénario 1, ce scénario permet également aux votants d'imprimer un reçu de bulletin de vote sécurisé une fois que leur vote a été exprimé par voie électronique pour tenir lieu de preuve physique pour le votant.

Avantages

- Le vote par ordinateur permet un degré de sécurité élevé en assurant une protection de bout en bout. Les terminaux de votation sont contrôlés et un réseau privé peut être utilisé.
- Permet à Élections Ontario de contrôler les environnements physique et informatique pour offrir un niveau élevé de facilité d'utilisation et d'accessibilité.
- Il est possible de régler les problèmes d'accessibilité concernant la saisie du mot de passe avec l'aide d'un membre du personnel de scrutin.
- L'authentification basée sur un mot de passe ne nécessite pas un système centralisé de liste électorale pour éviter les votes en double (sauf si ce scénario est combiné à d'autres modes).

Inconvénients

- Nécessite un effort de logistique important pour préparer, déployer et déclasser l'équipement de vote en réseau.
- Nécessite une formation spécialisée pour les membres du personnel de scrutin, le personnel de soutien et les équipes techniques comptant des unités supplémentaires, et ainsi de suite.
- Nécessite un mécanisme ou une procédure de remise de mots de passe aux votants.
- L'identification des votants repose sur la sécurité du processus de remise du mot de passe, qui n'est pas aussi sécurisé qu'un mécanisme basé sur l'identification physique.
- Les votants doivent quand même visiter un bureau de vote pour voter, sauf si cette option est combinée à un scénario de vote à distance.

Risques

- Dépend du courant et des infrastructures de réseautage disponibles dans chaque bureau de vote.
- Repose sur le système de remise du mot de passe pour assurer l'identité et l'admissibilité de l'électeur.

5.4 SCÉNARIO 4 : VOTE SUR SITE PAR TÉLÉPHONE AVEC AUTHENTIFICATION BASÉE SUR UN MOT DE PASSE

VOTE SUR SITE PAR TÉLÉPHONE AVEC AUTHENTIFICATION BASÉE SUR UN MOT DE PASSE

Comme dans le scénario, 2, les votants se présentent à un bureau de vote pour exprimer leurs suffrages sur site à l'aide d'un système téléphonique; toutefois, comme dans le scénario 3, l'authentification basée sur un mot de passe permet aux votants de se rendre directement au terminal de votation sans montrer de preuve d'identité à un membre du personnel de scrutin. Les votants saisissent leur mot de passe unique (avec l'aide d'un membre du personnel de scrutin si nécessaire) et sont authentifiés par le système, qui détermine leur admissibilité à voter.

Comme le décrit le scénario 2, un système téléphonique nécessitera un mot de passe numérique sous forme de numéro d'identification du votant (NIV) qui est utilisé pour authentifier l'utilisateur et activer le bulletin de vote sonore. Ce NIV doit être distribué au moyen d'un mode de remise qui établit un équilibre entre la commodité et la sécurité, et fournit des mesures de contrôle précises permettant de s'assurer que chaque votant obtient un seul NIV.

Les systèmes téléphoniques ne peuvent fournir une copie papier du bulletin de vote déposé.

Avantages

- Procure un niveau de sécurité de moyen à élevé, mais ne peut offrir a) une protection de bout en bout complète ou b) la sécurité d'une identification physique (voir les inconvénients).
- La facilité d'utilisation et l'accessibilité peuvent être très bonnes pour les votants ayant un handicap visuel, si ces personnes peuvent avoir recours aux membres du personnel de scrutin pour les aider à saisir le mot de passe.
- Le vote par téléphone est la façon la moins coûteuse (sur le plan de la logistique et des frais) d'offrir le vote en réseau dans les bureaux de vote; toutefois, quant au serveur, sa variabilité est bien moindre que dans le cas du vote par internet (le même serveur peut prendre en charge plus de votants par internet que de votants par téléphone).
- Ne nécessite pas un système centralisé de liste électorale au bureau de scrutin pour éviter les votes en double, si utilisé seul ou avec un mode intégré de vote en réseau.

Inconvénients

- Le vote sur site par téléphone nécessite un effort de logistique important pour préparer, déployer et déclasser l'équipement de vote en réseau, vérifier les lignes téléphoniques, la couverture du réseau cellulaire, et les réseaux (en particulier si le VOIP est utilisé).
- Nécessite également une formation spécialisée pour les membres du personnel de scrutin, le personnel de soutien et les équipes techniques comptant des unités supplémentaires, et ainsi de suite.
- Nécessite un mécanisme ou une procédure de remise des mots de passe/NIV aux votants.
- L'authentification du votant repose sur l'intégrité du processus de remise du NIV, qui n'est pas aussi sécurisé qu'un mécanisme basé sur des cartes d'identité physiques.
- Les votants doivent quand même visiter un bureau de vote pour voter (sauf si ce scénario est combiné à un scénario de vote à distance).
- Il est impossible d'obtenir une sécurité de bout en bout sans taxer considérablement la facilité d'utilisation : bien que les terminaux de votation soient contrôlés par le responsable de l'élection, les données qui quittent le téléphone ne sont pas protégées contre les attaques externes pouvant survenir dans le réseau (RTCP, cellulaire, etc.) ou par des attaques internes dans le système RVI.
- Non accessible pour les votants ayant un handicap auditif ou des handicaps moteurs graves.
- Le processus qui consiste à exprimer des suffrages est beaucoup plus long qu'au moyen d'un système informatique.

Risques

- Dépend de l'infrastructure téléphonique/de la couverture qui existent dans chaque bureau de vote et du courant et de l'infrastructure de réseautage en cas d'utilisation de VoIP.
- Possibilité d'attaques de type « intermédiaire » ou de mystification lors d'une séance de vote pendant que les données sont dans le RTCP.
- Repose sur le système de remise de mot de passe pour assurer l'identité et l'authenticité du votant.

5.5 SCÉNARIO 5 : VOTE À DISTANCE PAR TÉLÉPHONE AVEC AUTHENTIFICATION BASÉE SUR UN MOT DE PASSE

VOTE À DISTANCE PAR TÉLÉPHONE AVEC AUTHENTIFICATION BASÉE SUR UN MOT DE PASSE

Dans ce scénario, les électeurs peuvent voter à partir de n'importe quel endroit, pourvu qu'ils aient accès à un téléphone, qui peut être un téléphone conventionnel, un téléphone mobile, ou une voix sur IP (VOIP) à partir d'un ordinateur ou d'un téléphone. Les votants composent un numéro sans frais, choisissent la langue qu'ils privilégient, puis saisissent un mot de passe déterminé à l'avance à l'aide d'un clavier. Le système lui-même authentifie le votant et établit son admissibilité à voter. Si l'authentification est approuvée, le votant aura accès à un bulletin de vote sonore.

Comme le décrivent les scénarios 2 et 4, un système téléphonique nécessitera un mot de passe numérique sous forme de numéro d'identification du votant (NIV). Ce NIV doit être distribué au moyen d'un mode de remise qui établit un équilibre entre la commodité et la sécurité, et fournit des mesures de contrôle précises permettant de s'assurer que chaque votant obtient un seul NIV.

Les systèmes téléphoniques ne peuvent fournir de copie papier du bulletin de vote déposé.

Avantages

- Procure un niveau de sécurité de moyen à élevé, mais ne peut offrir a) une protection de bout en bout complète ou b) la sécurité d'une identification physique (voir les inconvénients).
- La facilité d'utilisation et l'accessibilité peuvent être très bonnes pour les votants ayant un handicap visuel, pourvu que le NIV soit suffisamment lisible par les personnes handicapées, ou qu'une personne puisse leur lire le NIV et/ou le saisir sur le clavier du téléphone (au besoin).
- Les votants peuvent participer à partir de n'importe quel téléphone. Ceux-ci sont disponibles dans presque toute l'Ontario et peuvent être utilisés par des votants de tout niveau de connaissance technique.
- Si un numéro sans frais est offert, les votants n'auront pas à payer l'appel.
- Les attaques entraînant un refus de service sont moins efficaces dans ce scénario que dans les scénarios 2 ou 4, car il y a de nombreux segments vulnérables (les liens entre chaque votant et le centre de données) et chacun transmet une petite proportion du total des votes.
- Si le lien entre un bureau de vote et le centre de données tombe, de nombreux votes sont touchés; par ailleurs, si la ligne résidentielle d'un votant est affectée, l'impact est beaucoup moins grand.

Inconvénients

- Nécessite un mécanisme/une procédure de remise des NIV aux votants.
- L'authentification du votant repose sur l'intégrité du processus de remise du NIV, qui n'est pas aussi sécurisé qu'un mécanisme fondé sur l'identification physique.
- Il est impossible d'obtenir une sécurité de bout en bout sans incidence importante sur la facilité d'utilisation : les terminaux de votation ne sont pas contrôlés par le responsable de l'élection et les données qui quittent le téléphone ne sont pas protégées contre les attaques externes pouvant survenir dans le réseau (RTCP, cellulaire, etc.) ou par des attaques internes dans le système RVI.
- Non accessible aux votants ayant un handicap auditif et/ou un moteur graves.
- Pas aussi convivial qu'une interface informatique.
- Le processus qui consiste à exprimer des suffrages est plus long que le processus de vote par interface informatique.
- L'infrastructure centrale (le système RVI) n'est pas aussi bien adaptable que l'infrastructure web.
- Les numéros sans frais constituent un coût opérationnel ajouté.

Risques

- Les lignes téléphoniques requises pour voter peuvent être facilement saturées si elles ne sont pas d'une taille appropriée.
- Possibilité d'attaques de type « intermédiaire » ou de mystification lors d'une séance de vote pendant que les données sont dans le RTCP.
- Repose sur le système de remise de mot de passe pour assurer l'identité et l'authenticité du votant.

5.6 SCÉNARIO 6 : VOTE À DISTANCE PAR ORDINATEUR, PAR INTERNET, AVEC AUTHENTIFICATION BASÉE SUR UN MOT DE PASSE

VOTE À DISTANCE PAR ORDINATEUR, PAR INTERNET, AVEC AUTHENTIFICATION BASÉE SUR UN MOT DE PASSE

Dans ce scénario, les électeurs peuvent voter à partir de n'importe quel endroit, pourvu qu'ils aient un ordinateur (muni du logiciel approprié) et un accès à internet. Les votants accèdent généralement à un site web de vote au moyen d'un navigateur web et saisissent un mot de passe qui authentifie leur identité dans le système de vote. Le système vérifie leur identité et leur admissibilité à voter, puis affiche un bulletin de vote en ligne. L'autorisation d'accéder au système de vote permet tout genre de système basé sur un mot de passe, et non seulement les systèmes numériques.

Comme dans tout système de vote à distance qui repose sur des mots de passe à des fins d'authentification, la remise de mots de passe doit établir un équilibre entre la commodité et la sécurité. Des mesures de contrôle particulières doivent être utilisées pour veiller à ce que chaque votant obtienne un seul mot de passe.

Ce scénario permet aux votants d'imprimer un accusé de réception de bulletin de vote sécurisé à titre de preuve matérielle du votant lorsqu'ils ont voté électroniquement. Il pourrait être combiné à un mode de scrutin sur site si nécessaire. Si le vote à distance par ordinateur a lieu parallèlement au vote sur site par ordinateur, il faudra disposer d'une liste électorale centralisée pouvant être accessible et mise à jour à partir du bureau de scrutin pour éviter les votes en double.

Avantages

- Le vote à distance par ordinateur offre un degré très élevé de sécurité, à l'exception du processus d'identification du votant (voir les inconvénients).
- Il est possible d'obtenir la sécurité de bout en bout par le chiffrement, ce qui permet d'appliquer des mesures protectrices contre les attaques externes et internes.
- La facilité d'utilisation et l'accessibilité peuvent être très bonnes pour les votants, peu importe leur type de handicap, pourvu qu'ils soient familiers avec les ordinateurs et qu'ils possèdent les interfaces d'accessibilité requises.
- Les votants peuvent participer à partir de n'importe quel ordinateur possédant un accès à internet, ce qui signifie que la presque totalité des ontariens ont un accès. Il est possible de voter non seulement à partir de la maison, mais également d'endroits comme les lieux de travail, des bibliothèques ou des cafés internet (ce qui donne lieu à la fois à des risques et à des possibilités).
- Seule l'infrastructure centrale est requise; il n'existe pas d'exigences d'autres composantes au niveau du serveur ou du bureau de scrutin. Cette infrastructure peut être adaptée très efficacement, en comparaison avec d'autres modes de scrutin, en particulier le vote par téléphone.
- L'inscription en ligne et le processus de vote peuvent être très commodes et rapides (souvent moins de 5 minutes).

Inconvénients

- Le vote à distance reposant sur une authentification par mot de passe requiert un mécanisme de remise des mots de passe aux votants.
- L'authentification du votant repose sur l'intégrité du processus de remise du mot de passe/du NIV, qui n'est pas aussi sécurisé qu'un mécanisme fondé sur des documents d'identification physique.
- Les votants pourraient devoir acquitter les coûts de l'accès à internet.
- Seuls les votants qui ont accès à des ordinateurs et qui sont rompus à l'utilisation de ceux-ci peuvent utiliser facilement ce mode de scrutin. C'est la même chose dans le cas des votants handicapés : seuls ceux qui savent comment naviguer sur internet pourront voter avec facilité.

- Il n'y a pas de contrôle de la sécurité ou de la stabilité des ordinateurs utilisés par les votants pour voter (virus, logiciels malveillants, etc.).

Risques

- Possibilité d'attaques entraînant un refus de service, car les serveurs de l'élection sont accessibles par internet.
- Absence de contrôle sur les spécifications des ordinateurs des votants.
- Certains groupes de la population ne se montreront peut-être pas très enthousiastes face à la perspective d'avoir recours à ce mécanisme à cause du fossé numérique :
    - Les votants qui ne sont pas habitués à utiliser les ordinateurs.
    - Les votants handicapés qui ne sont pas rompus à l'utilisation des ordinateurs et/ou qui n'ont pas d'interfaces d'accessibilité.
- Repose sur le système de remise de mot de passe pour assurer l'identité et l'authenticité du votant.

5.7 SCÉNARIO 7 : VOTE À DISTANCE PAR TÉLÉPHONE MOBILE, PAR INTERNET, AVEC AUTHENTIFICATION BASÉE SUR UN MOT DE PASSE

VOTE À DISTANCE PAR TÉLÉPHONE MOBILE, PAR INTERNET, AVEC AUTHENTIFICATION BASÉE SUR UN MOT DE PASSE

Dans ce scénario, les votants peuvent voter de partout, pourvu qu'ils aient un téléphone mobile convenable (voir ci-après) qui peut nécessiter un logiciel particulier et un accès à internet. Une fois que les électeurs ont accès à l'application ou au site internet approprié au moyen d'un téléphone, ils saisissent un mot de passe pour se faire authentifier. Si le votant est admissible, le système affiche automatiquement les options de vote. Il est possible d'obtenir une autorisation d'accéder au système de vote en utilisant n'importe quel genre de système basé sur un mot de passe; toutefois, les mots de passe numériques sont privilégiés, car ce ne sont pas tous les téléphones mobiles qui sont munis d'un clavier complet.

Comme dans le cas des scénarios précédents basés sur un mot de passe, les mots de passe doivent être distribués au moyen d'un mode de remise qui établit un équilibre entre la commodité et la sécurité, et qui comporte des mesures de contrôle particulières qui assurent que chaque votant obtient un seul mot de passe.

Le dispositif utilisé pour voter peut être presque n'importe quel téléphone mobile, pourvu qu'il puisse prendre en charge soit une application sur mesure soit un navigateur web approprié. Compte tenu des limites de la taille de l'écran, du pouvoir de l'unité centrale, des éléments du système d'exploitation et du clavier de nombreux téléphones mobiles standards, les appareils les mieux adaptés à cette fin sont les téléphones intelligents; toutefois, le taux de pénétration de ces appareils est faible comparativement à l'ensemble du marché de la téléphonie cellulaire (généralement inférieur à 30 %), et ce ne sont pas tous les utilisateurs qui connaissent les caractéristiques de pointe, comme les applications.

Que le vote ait lieu au moyen d'un navigateur web ou d'une application sur mesure, les votants doivent acquitter les frais liés à la connexion internet. De plus, l'accessibilité est essentiellement fonction des capacités intégrées fournies par l'appareil lui-même, qui sont très limitées comparativement aux options qu'offrent les ordinateurs.

Ce scénario peut être combiné à un mode de scrutin sur site au besoin. Selon les besoins de vote sur site, il faudra vraisemblablement disposer d'une liste électorale centralisée pouvant être accessible et mise à jour à partir du bureau de scrutin pour éviter les votes en double.

Pour appuyer la vérifiabilité individuelle, le système peut être conçu de manière à fournir une copie d'accusé de réception pour aider les votants à vérifier que leurs bulletins de vote ont été dénombrés par le responsable de l'élection.

Avantages

- Le vote à distance sur internet par téléphone mobile peut offrir un niveau élevé de sécurité, à l'exception, peut-être, de l'identification du votant (voir les inconvénients).
- Il est possible d'obtenir de la sécurité de bout en bout, ce qui permet d'appliquer des mesures protectrices contre les attaques externes et internes.
- Les votants peuvent voter de n'importe quel endroit où un réseau de téléphonie cellulaire de deuxième génération ou plus est accessible (plus de 95 % de la province).
- Les téléphones mobiles sont moins susceptibles d'être contaminés par des logiciels malveillants ou des virus que les ordinateurs.
- Seule l'infrastructure centrale obligatoire est requise; aucune composante supplémentaire n'est nécessaire au niveau du serveur ou du bureau de vote. Cette infrastructure peut être constituée de manière à être adaptée très efficacement (comparativement aux autres modes de scrutin).

Inconvénients

- La facilité d'utilisation et l'accessibilité sont négligeables et dépendent complètement des caractéristiques du téléphone cellulaire. Seuls les téléphones intelligents les plus récents offrent des niveaux vraiment acceptables de facilité d'utilisation de l'interface.
- Nécessite un mécanisme/une procédure de remise des mots de passe aux votants.
- L'identité des votants repose sur le processus de remise des mots de passe, qui n'est pas aussi sécurisé que le mécanisme basé sur une identification physique.
- Les votants devront acquitter les frais liés à l'accès à internet.
- Uniquement pour les votants qui sont habitués de naviguer sur internet et/ou d'utiliser des applications de téléphones mobiles.
- il existe une possibilité d'attaques entraînant un refus de service, car les serveurs de l'élection sont accessibles par internet.
- Nécessite des efforts supplémentaires pour développer des plateformes pour appareils multiples (y compris l'impact correspondant sur la mise à l'essai et le soutien).

Risques

- Possibilité d'attaques entraînant un refus de service.
- Certaines parties de la population seraient moins désireuses d'utiliser ce mécanisme :
    - Les votants qui utilisent des téléphones mobiles standards.
    - Les votants qui ne sont pas rompus aux fonctionnalités du téléphone intelligent.
    - Les votants handicapés.
- La multiplicité des applications pour divers téléphones/fureteurs fait augmenter la demande de soutien et les frais connexes.
- Repose sur le système de remise de mot de passe pour assurer l'identité et l'authenticité du votant.

5.8 SCÉNARIO 8 : VOTE SUR SITE PAR ORDINATEUR, AVEC AUTHENTIFICATION BASÉE SUR LES SYSTÈMES TIERS EXISTANTS

VOTE SUR SITE PAR ORDINATEUR, AVEC AUTHENTIFICATION BASÉE SUR LES SYSTÈMES TIERS EXISTANTS

Dans ce scénario, les votants se présentent à un bureau de vote et vont directement au terminal de votation, où ils s'authentifient auprès du système de vote au moyen d'un site web tiers (comme ServiceOntario). Une fois que les votants ont été identifiés, ils sont réorientés vers le portail de scrutin où ils seront autorisés à voter.

Les membres du personnel de scrutin n'ont à poser aucun geste dans le cadre de ce scénario, si ce n'est de superviser le processus de scrutin et d'aider les votants sur demande.

Comme l'authentification comporte une interaction avec un site tiers, la sécurité et l'accessibilité sont fonction des normes établies pour ce site. Il doit donc impérativement s'agir de sites tiers dignes de confiance et très sécurisés offrant les options d'accessibilité nécessaires.

Ce scénario peut être combiné à un mode de scrutin à distance sans qu'il soit nécessaire de disposer d'une liste électorale centralisée dans les bureaux de vote, car le contrôle exercé sur les votants pour éviter les votes en double est fait par le système de vote lui-même.

Comme dans les autres scénarios basés sur un ordinateur, ce scénario permet également aux votants d'imprimer un accusé de réception de bulletin de vote sécurisé comme preuve matérielle pour le votant une fois qu'ils ont exprimé leur suffrage par voie électronique.

Avantages

- La sécurité est élevée, car la protection de bout en bout peut être assurée, les terminaux de votation sont contrôlées, et un réseau privé peut être utilisé.
- La facilité d'utilisation et l'accessibilité peuvent être très bonnes selon la configuration des bornes interactives et les normes de l'authentificateur tiers (ce qui exclut la saisie du mot de passe, qui peut nécessiter de l'aide d'un membre du personnel de scrutin).

- Ne nécessite pas une liste électorale centralisée pour éviter les votes en double. Le système de vote lui-même gère cette situation.

Inconvénients

- Nécessite un effort de logistique important pour préparer, déployer et déclasser l'équipement de vote en réseau.
- Nécessite une formation spécialisée pour les membres du personnel de scrutin, le personnel de soutien et les équipes techniques comptant des unités supplémentaires, et ainsi de suite.
- Nécessite une intégration avec les sites tiers. L'intégration rendrait nécessaire des évaluations détaillées des niveaux de sécurité tiers et des procédures.
- L'identification des votants repose sur les systèmes tiers, qui doivent être dignes de confiance et ne sont pas aussi sécurisés qu'un mécanisme fondé sur des identifications physiques.
- Seuls les votants ayant accès à ces systèmes tiers pourraient voter au moyen du système en réseau.
- Les votants doivent quand même visiter un bureau de vote pour voter, sauf si cette option est combinée à un scénario de vote à distance.

Risques

- Dépendance à l'égard du courant et des infrastructures de réseautage dans les bureaux de vote.
- Repose sur les systèmes tiers pour assurer l'identité et l'authenticité du votant.
- Participation limitée aux votants qui peuvent avoir accès aux systèmes tiers.

5.9 SCÉNARIO 9 : VOTE À DISTANCE PAR ORDINATEUR, PAR INTERNET, AVEC AUTHENTIFICATION BASÉE SUR DES TIERS

VOTE À DISTANCE PAR ORDINATEUR, PAR INTERNET, AVEC AUTHENTIFICATION BASÉE SUR DES TIERS

Dans ce scénario, les votants peuvent voter à partir de n'importe quel endroit, pourvu qu'ils aient un ordinateur (muni du logiciel approprié) et un accès à internet. Ils s'authentifieront auprès du système de vote au moyen d'un site web tiers de confiance. Une fois que les votants ont été identifiés, ils sont réorientés vers le portail de scrutin où ils seront autorisés à voter.

Tel qu'il est mentionné au scénario 8, ce mécanisme d'authentification sous-tend implicitement que le responsable de l'élection fait confiance aux mécanismes utilisés par les tiers participants pour authentifier leurs utilisateurs. Par conséquent, il conviendrait de considérer que certains types d'évaluation et/ou de vérification valident le processus utilisé pour identifier les utilisateurs de façon suffisamment sécurisée.

Avantages

- Le niveau de sécurité peut être très élevé, quoique le système fasse confiance aux mécanismes d'authentification des tiers et aux ordinateurs des votants (voir les inconvénients).
- Il n'est pas nécessaire d'établir des processus complexes de remise de justificatifs d'identité en vue du scrutin (p. ex. des mots de passe) aux votants, car les tiers s'en occupent.
- La sécurité de bout en bout est possible, ce qui permet d'appliquer des mesures de protection pour faire face aux attaques externes et internes.
- La facilité d'utilisation et l'accessibilité peuvent être très bonnes pour les votants, peu importe leur type de handicap, pourvu qu'ils soient rompus à l'utilisation des ordinateurs et qu'ils aient les composantes d'accessibilité requises; toutefois, les tiers doivent également fournir des sites accessibles.
- Les votants peuvent participer à partir de tout ordinateur disponible offrant un accès internet, soit près de 100 % de la région. Cela comprend notamment les lieux de travail, les bibliothèques et les cafés internet.
- Seule l'infrastructure centrale obligatoire est requise; aucune composante supplémentaire n'est nécessaire au niveau du serveur ou du lieu de vote. Cette infrastructure peut être établie pour être adaptée très efficacement (en comparaison avec les autres modes de scrutin).
- Le processus de vote peut être très commode et rapide (moins de 5 minutes).
- Ne nécessite pas un système de liste électorale centralisée pour éviter les votes en double. Le système de vote lui-même gère cette situation.

Inconvénients

- Nécessite différentes intégrations avec des sites tiers. L'intégration exigerait des évaluations détaillées des niveaux et des procédures de sécurité suivies par le tiers.
- L'identification des votants repose sur les systèmes tiers, qui doivent être dignes de confiance et ne sont pas aussi sécurisés qu'un mécanisme fondé sur des identifications physiques.
- Seuls les votants ayant accès à ces systèmes tiers pourraient voter au moyen du système en réseau.
- Les votants devront acquitter les frais liés à l'accès à internet.
- Seuls les votants rompus à l'utilisation des ordinateurs, notamment ceux qui sont handicapés, peuvent avoir recours à ce mode de scrutin.
- Il est plus facile de commettre des attaques entraînant un refus de service dans ce scénario.
- Il n'y a pas de contrôle sur les ordinateurs utilisés par les votants pour exprimer leurs suffrages.

Risques

- Les attaques entraînant un refus de service et l'absence de contrôle sur les ordinateurs des votants.
- Certaines parties de la population seraient moins désireuses d'utiliser ce mécanisme :

- Les votants qui ne sont pas à l'aise avec les ordinateurs.
- Les votants handicapés qui ne sont pas rompus à l'utilisation des ordinateurs et/ou qui n'ont pas de composantes d'accessibilité.
- Les votants qui n'ont de lien avec aucun des tiers utilisés à des fins d'authentification.
- Repose sur les systèmes tiers pour assurer l'identité et l'authenticité du votant.

5.10 SCÉNARIO 10 : VOTE À DISTANCE PAR TÉLÉPHONE MOBILE, PAR INTERNET, AVEC AUTHENTIFICATION BASÉE SUR DES TIERS

VOTE À DISTANCE PAR TÉLÉPHONE MOBILE, PAR INTERNET, AVEC AUTHENTIFICATION BASÉE SUR DES TIERS

Dans ce scénario, les votants peuvent voter à partir de n'importe quel endroit, pourvu qu'ils aient un téléphone mobile avec navigateur web et un accès à internet. Ils s'authentifient dans le système de vote en choisissant un site web tiers, qui leur demandera de s'identifier eux-mêmes. Une fois que les votants ont été identifiés, ils sont réorientés vers le portail de scrutin où ils seront autorisés à voter.

Comme dans les scénarios 8 et 9, ce mécanisme d'authentification sous-tend implicitement que le responsable de l'élection fait confiance aux mécanismes utilisés par les tiers participants pour authentifier leurs utilisateurs, et que ce site tiers est compatible avec les téléphones mobiles acceptés.

La détermination de l'admissibilité du votant a lieu au système de vote (le tiers est seulement chargé de l'identification de l'utilisateur). Cette approche évite d'avoir à partager la liste électorale avec les tiers.

Ce scénario présente des problèmes de facilité d'utilisation parce qu'il est plutôt complexe de naviguer dans divers sites web avec un téléphone mobile, notamment parce que certains sites tiers ne sont peut-être pas adaptés aux appareils mobiles.

Avantages

- Les votants peuvent participer à l'aide de certains appareils mobiles, et peuvent se trouver à n'importe quel endroit où un réseau cellulaire de deuxième génération ou plus récent est accessible.
- Le niveau de sécurité peut être très élevé, quoique le système fasse confiance aux mécanismes d'authentification des tiers et aux terminaux mobiles des votants (voir les inconvénients).
- Les téléphones mobiles sont moins susceptibles d'être contaminés par des logiciels malveillants.
- Seule l'infrastructure centrale obligatoire est requise; il n'y a aucune exigence supplémentaire sur le plan des composantes au niveau du serveur ou du bureau de scrutin. Cette infrastructure peut être établie pour être adaptée très efficacement (en comparaison avec les autres modes de scrutin).

- Il n'est pas nécessaire d'établir des processus complexes de remise de justificatifs d'identité en vue du scrutin (p. ex. des mots de passe) aux votants, car les tiers s'en occupent.
- Ne nécessite pas un système de liste électorale centralisée pour éviter les votes en double. Le système de vote lui-même gère cette situation.

Inconvénients

- Il est impossible de réaliser une sécurité de bout en bout en raison des restrictions du réseau et du recours à des tiers, ce qui ouvre la voie à des attaques internes.
- La facilité d'utilisation et l'accessibilité dépendent complètement des caractéristiques du téléphone cellulaire. Seuls les téléphones intelligents les plus nouveaux offrent des interfaces acceptables sur le plan de la facilité d'utilisation, mais l'accessibilité est très limitée.
- Les votants devront acquitter les frais liés à l'accès à internet.
- Seuls les votants qui possèdent ces genres d'appareils peuvent utiliser ce mode de scrutin.
- Il est plus facile de commettre des attaques entraînant un refus de service dans ce scénario, car l'accès aux serveurs de l'élection repose sur des portails internet standards.
- Nécessite des efforts supplémentaires pour développer des plateformes pour appareils multiples (y compris l'impact correspondant sur la mise à l'essai et le soutien).
- Nécessite une intégration avec les sites tiers. L'intégration nécessiterait des évaluations détaillées sur les niveaux et les procédures de sécurité suivis par ces tiers.
- L'identification des votants repose sur des systèmes tiers, qui doivent être dignes de confiance et ne sont pas aussi sécurisés qu'un mécanisme fondé sur des identifications physiques.
- Seuls les votants ayant accès à ces systèmes tiers pourraient voter au moyen du système en réseau.

Risques

- possibilité d'attaques entraînant un refus de service.
- certaines parties de la population seraient moins désireuses d'utiliser ce mécanisme :
    - Les citoyens qui ne possèdent pas de téléphones intelligents.
    - Les votants qui sont handicapés.
    - Les votants qui n'ont de lien avec aucun des tiers utilisés à des fins d'authentification.
- Nombre d'options font augmenter le degré de difficulté et le coût de leur prise en charge.
- Repose sur les systèmes tiers pour assurer l'identité et l'authenticité du votant.

5.11 RÉSULTATS DE LA RECHERCHE : LISTE DES SCÉNARIOS RETENUS

Compte tenu du résultat de la recherche sur le vote en réseau, les scénarios 7, 8, 9 et 10 ont cessé d'être pris en compte pour les motifs suivants :

Le scénario 7, qui repose sur une plateforme de téléphone mobile/internet et de téléphone intelligent, obtient un faible pointage en regard des critères d'accessibilité.

Les scénarios 8 et 9, qui obtiennent un pointage comparable aux autres scénarios de vote par ordinateur, doivent être éliminés car à l'heure actuelle, un système ou service d'authentification par un tiers n'est pas disponible en Ontario. Cependant, cette option devrait être étudiée dans l'avenir, car la situation peut changer.

Le scénario 10, qui repose également sur la plateforme de téléphone mobile par internet, obtient un mauvais pointage sur le plan de l'accessibilité.

SIX DES DIX SCÉNARIOS ÉLIMINÉS

Les scénarios 3 et 4, qui ont obtenu un bon pointage à l'évaluation, ont été éliminés à la suite d'une consultation, car le fait d'exiger des électeurs qu'ils s'inscrivent au préalable et qu'ils soumettent un mot de passe à un bureau de vote créait un obstacle superflu sans procurer d'avantage substantiel aux votants.

Il reste quatre scénarios (1, 2, 5 et 6) qui pourraient en conséquence faire l'objet d'un projet pilote et constituer la liste des scénarios retenus, qui seraient évalués davantage dans la présente étude de cas :

LISTE DES QUATRE MODES RETENUS

SCÉNARIO	LIEU	PLATEFORME	AUTHENTIFICATION
1	Sur site	Ordinateur	Identification physique
2	Sur site	Téléphone	Identification physique
5	À distance	Téléphone	Mot de passe
6	À distance	Ordinateur	Mot de passe

Comme chacun de ces scénarios procure un ensemble d'avantages unique, la présente étude de cas mesure comment ces quatre modes peuvent être combinés en un seul modèle qui :

- Inclut le vote sur site et à distance par téléphone;
- Inclut le vote sur site et à distance par ordinateur;
- Utilise une identification physique pour authentifier les votants sur site;
- Utilise une combinaison d'inscription préalable et d'authentification par mot de passe pour le vote à distance;
- Offre un bulletin de vote sur papier avec l'utilisation de la méthode actuelle d'authentification des votants.

AVANTAGES DU VOTE SUR SITE EN RÉSEAU

En offrant des options de vote sur site en réseau, ce modèle peut authentifier les votants au moyen d'une méthode qui est non seulement la plus sécurisée, mais qui est également connue des votants. Un votant n'aurait pas besoin de faire son inscription préalable pour un vote en réseau avant de voter sur site par ordinateur ou par téléphone; il n'a qu'à présenter une pièce d'identité pour qu'un membre du personnel de scrutin lui donne accès à l'appareil de vote. Bien qu'il s'agisse de la solution la plus simple pour le votant, elle est aussi relativement complexe pour Élections Ontario sur le plan de la formation du membre du personnel de scrutin, de la mise en œuvre de l'infrastructure, et de l'élaboration du système.

AVANTAGES DU VOTE À DISTANCE EN RÉSEAU

En offrant des options de vote à distance, qui peuvent être authentifiées au moyen d'un processus fondé sur un mot de passe, ce modèle peut présenter les avantages uniques du vote à distance. Les votants peuvent voter à la maison ou sur leur lieu de travail et se servir du téléphone ou de l'internet, selon le mode qui est le plus commode ou accessible pour eux, et ils peuvent le faire très rapidement.

Le prochain chapitre décrit en détails comment ces quatre modes peuvent être mis en œuvre dans un projet pilote d'élections Ontario.

6. REVUE DES SCÉNARIOS RETENUS

Le présent chapitre constitue une revue, fondée sur le processus, de la façon dont les quatre modes retenus pourraient être mis en œuvre dans un projet pilote d'élections Ontario. Les détails à cet égard reposent sur une évaluation des activités actuelles d'élections Ontario. Les processus décrits dans le présent chapitre sont conçus pour étayer les principes fondamentaux d'élection retenus pour orienter cette initiative et pour fonctionner dans le contexte des besoins et des restrictions propres au contexte actuel de l'Ontario.

Les conclusions de la recherche ont établi une liste des quatre modes de scrutin en réseau retenus : le vote sur site, par téléphone, le vote sur site, par ordinateur, le vote à distance, par téléphone, et le vote à distance, par ordinateur. Afin de dresser un portrait clair de la façon dont ces quatre modes pourraient être mis en œuvre dans un projet pilote d'élections Ontario, le présent chapitre décrit leur mise en œuvre en exposant les cinq étapes du processus de vote :

1. **Inscription et authentification**

   Les éléments et les processus nécessaires pour établir la liste des électeurs, les inscrire au vote en réseau, prouver leur identité, et valider leur admissibilité à voter.

2. **Vote**

   Les éléments et les processus nécessaires pour permettre aux votants de voter au moyen des modes de scrutin en réseau.

   Il y a trois sujets clés : le vote sur site; le vote à distance et le registre du scrutin électronique.

3. **Archivbage de votes**

   Les processus requis pour gérer de façon sûre et exacte l'archivage et la gestion des bulletins de vote dans le système de vote en réseau une fois qu'ils ont été déposés.

4. **Compilation**

   Les éléments et les processus nécessaires pour compiler et déclarer les résultats dans le contexte du vote en réseau et les grouper avec les résultats de la filière conventionnelle une fois que la période de scrutin est terminée.

5. **Vérification**

   Les éléments et les processus qui doivent exister pour étayer la vérification externe.

   La capacité de vérifier et de revoir le système de vote en réseau est cruciale pour établir la transparence recommandée par cette étude de cas.

Comme il serait possible d'intégrer les quatre modes dans le contexte d'un projet pilote, la section qui suit donne un aperçu de la façon de les mettre en œuvre dans un modèle intégré. La faisabilité de chacun des modes sera mesurée dans les sections ultérieures.

APERÇU

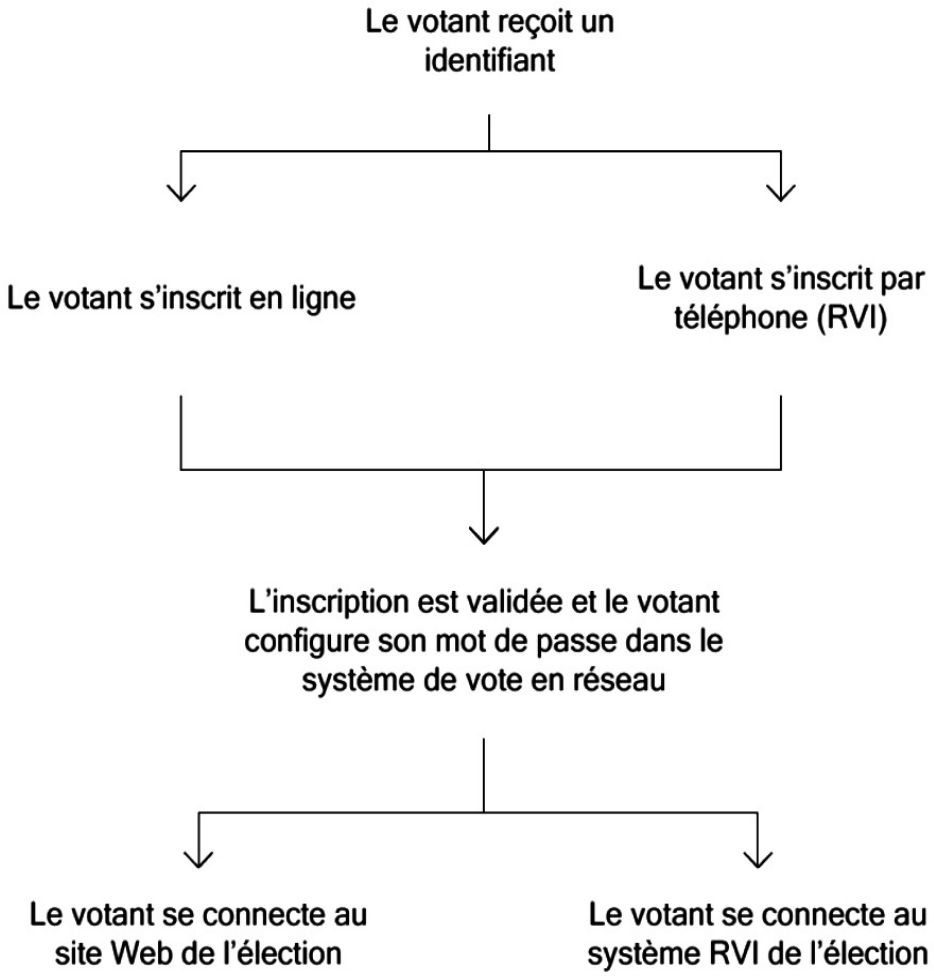
NOUVEAUX PROCESSUS ET NOUVELLES TECHNOLOGIES

Voici un aperçu de ce modèle intégré, structuré conformément aux cinq étapes ci-dessus. Pour chaque étape, l'aperçu décrit, à un haut niveau, comment les différentes parties prenantes (votants, membres du personnel de scrutin, personnel du bureau central d'élections Ontario, etc.) interagiront avec les nouveaux processus et les nouvelles technologies nécessaires pour soutenir le vote en réseau. Il est davantage question de chaque étape du processus de vote dans les sous-sections sur la façon de procéder.

Bien que l'on puisse faire référence à certains besoins et risques ou à certaines stratégies d'atténuation du risque clés, ces sujets sont abordés de manière plus exhaustive dans des sections et chapitres subséquents du présent document.

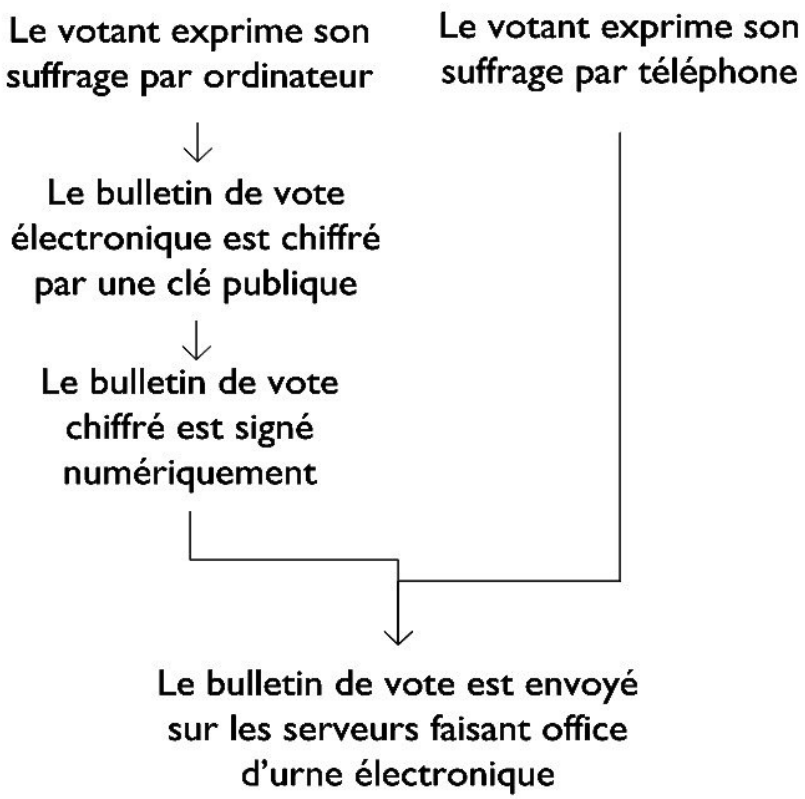
INSCRIPTION ET AUTHENTIFICATION

1. Tous les électeurs figurant dans la liste préliminaire des électeurs reçoivent un courrier d'inscription pour le vote en réseau comportant un identifiant numérique sécurisé personnel (ID d'électeur) et des instructions d'accès au site web d'inscription pour le vote en réseau à distance.
2. Les électeurs qui optent pour le vote en réseau à distance se rendent sur le site web et saisissent leur id d'électeur et leur date de naissance afin de s'inscrire. Pour plus de sécurité, le numéro du permis de conduire peut être utilisé pour vérifier leur identité. Un second courrier peut également être envoyé à ce stade pour fournir au votant un second numéro d'identification personnel (NIP) sécurisé avant de passer à l'étape suivante.
3. Après l'authentification, le système valide la qualité d'électeur de chacun et demande la configuration d'un mot de passe sécurisé à utiliser au moment du vote. éventuellement, les électeurs n'ayant pas facilement accès à internet peuvent appeler un numéro sans frais pour mener à bien la même procédure via une interface de réponse vocale intégrée (RVI) qui se connecte au même système dorsal.
4. Dès l'ouverture de la période de vote par anticipation, les votants inscrits pour le vote à distance peuvent se connecter au site web ou au système RVI de l'élection à l'aide de leur id d'électeur et de leur mot de passe.



VOTE

5. Une fois qu'un votant a été authentifié sur le site web de l'élection, il peut exprimer son suffrage en sélectionnant le candidat de son choix à l'écran. Les électeurs votant par téléphone feront leurs sélections via un système de menu automatisé. La facilité d'emploi et l'accessibilité de ces deux options doivent être optimisées afin d'offrir la meilleure expérience possible aux utilisateurs.
6. Après avoir voté par l'un de ces moyens, le votant est rayé de la liste des électeurs et reçoit un accusé de réception qui lui permettra de vérifier la prise en compte de son suffrage dans les résultats finaux de l'élection.
7. La liste des votants peut être gérée dans le cadre d'un processus en ligne en temps réel pour éviter l'éventualité d'un double vote via différents modes de scrutin et maintenir à jour le système de vote en réseau en fonction des révisions. Il serait aussi possible de cantonner les votants aux modes de scrutin à distance une fois leur inscription effectuée afin d'éviter tout risque de double vote.



ARCHIVAGE DES VOTES

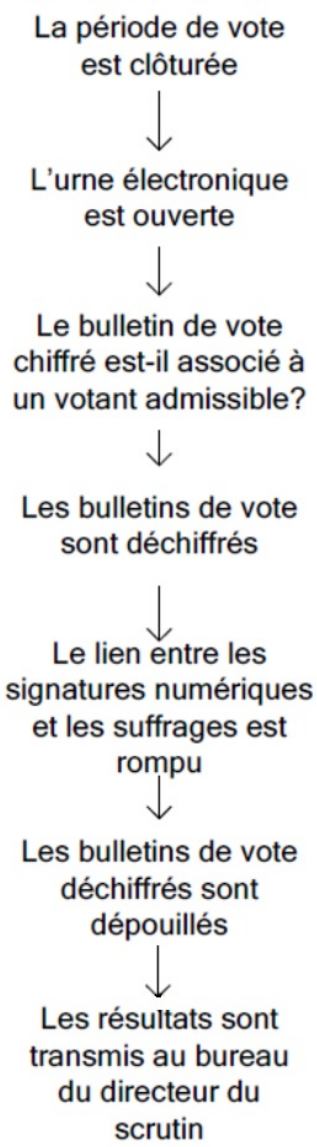
8. Une fois le suffrage exprimé par téléphone ou par ordinateur, le bulletin de vote électronique est archivé dans un environnement serveur sécurisé régi par des mesures de sécurité physiques et logicielles strictes et répondant à des exigences draconiennes en matière de disponibilité et de performance.
9. Ce bulletin de vote fait l'objet d'un chiffrement sécurisé empêchant la lecture de son contenu tant qu'il est archivé dans l'urne électronique.

COMPILATION

10. À la fin de la période de vote, les urnes électroniques sont transférées dans un environnement isolé et sécurisé en vue du dépouillement.
11. Avant le déchiffrement, le système vérifie que tous les bulletins de vote contenus dans les urnes ont été « déposés » par des personnes ayant les qualités requises pour voter.
12. Les bulletins de vote sont déchiffrés par les membres autorisés au sein du personnel d'élections Ontario, chacun d'entre eux étant en possession d'une partie de la clé nécessaire au déchiffrement.
13. Après le déchiffrement, les bulletins de vote ne peuvent pas être associés à un votant.
14. Le système compte les bulletins valides et communique les résultats combinés du vote en réseau au directeur du scrutin, qui les inclut au décompte officiel.

VÉRIFICATION

15. Le système doit permettre au conseil de gestion du vote en réseau de procéder à un nouveau déchiffrement et à une nouvelle compilation, le cas échéant, sous la supervision de vérificateurs indépendants.
16. Le système doit permettre aux vérificateurs indépendants de procéder à un nouveau décompte, en parallèle de la liste certifiée des bulletins de vote déchiffrés. Les vérificateurs doivent être en mesure de travailler à partir des bulletins de vote déchiffrés et d'obtenir des résultats traduits en clair susceptibles d'être comparés à ceux générés par le système.
17. Le système doit permettre aux vérificateurs indépendants de vérifier et de certifier l'intégrité et l'authenticité des composantes du système utilisées dans le traitement des urnes électroniques, y compris l'authenticité des logiciels, l'intégrité du système, l'intégrité et l'authenticité des fichiers journaux générés, etc.



6.1 AUTHENTIFICATION DU VOTANT

La capacité d'établir une identité de l'électeur de manière sécurisée et définitive constitue l'un des principes de base qui oriente cette initiative. Il s'agit d'une exigence démocratique fondamentale, qui représenterait par conséquent une composante technique et procédurale cruciale d'un projet pilote sur le vote en réseau. En ce qui concerne le vote en personne dans un bureau de scrutin, le mode d'authentification serait actuellement le suivant : présentation d'une identification physique à un membre du personnel de scrutin; toutefois, le vote à distance comporte un défi plus complexe.

Élections Ontario, qui ne peut actuellement miser sur une forme établie d'authentification électronique*, doit (au moins dans le cas du projet pilote) mettre en œuvre son propre mode autonome d'authentification des votants.

La présente section traite des flux des processus et des exceptions qui s'appliquent à trois processus d'authentification des votants :

- **L'authentification à distance standard**, dans le cadre de laquelle les électeurs s'inscrivent à l'avance aux modes de scrutin en réseau à distance au moyen d'une preuve d'identité.
- **Une authentification à distance autre,** dans le cadre de laquelle les électeurs s'inscrivent à l'avance au moyen d'un processus basé sur un portail avec deux envois postaux distincts.
- **L'authentification supervisée**, dans le cadre de laquelle un membre du personnel de scrutin d'Élections Ontario vérifie l'identité d'un votant et autorise celui-ci à se servir d'un dispositif de vote.

* l'une des façons les plus faciles pour Élections Ontario d'authentifier l'identité d'un votant à distance serait de lui demander de fournir de l'information que seul lui et Élections Ontario connaissent.

Toutefois, Élections Ontario a seulement accès à un éventail limité de données personnelles des votants, dont la plupart ne sont ni secrètes ni, par conséquent, sécurisées.

Élections Ontario pourrait également miser sur un mode sécurisé d'authentification à distance par un organisme gouvernemental tiers. Cependant, un tel mécanisme n'est pas suffisamment mûr ou répandu pour pouvoir être intégré à un système de vote en réseau.

Authentification à distance standard

Pour exprimer un suffrage à l'aide des modes de scrutin en réseau à distance (téléphone et ordinateur), les votants s'authentifieraient au moyen d'une combinaison formée d'un identificateur unique et d'un mot de passe. Pour ce faire, ils doivent d'abord s'inscrire au mode pertinent.

Compte tenu de l'équilibre à établir au niveau du besoin de l'électorat en matière de processus simple, le moyen le plus solide dont dispose Élections Ontario serait de confirmer l'identité de l'électeur *pendant* le processus d'inscription afin qu'au moment de la connexion et du vote, les justificatifs d'identité soient les plus sécurisés possibles.

Chaque étape du processus doit par conséquent établir un équilibre entre présenter le moins d'obstacles possible au votant et établir l'identité du votant de la façon la plus sécurisée possible, compte tenu des restrictions externes.

Le flux du processus serait le suivant :

1. Élections Ontario produit une liste des électeurs qui est importée dans le système de vote en réseau et mise à la disposition des dispositifs et du logiciel du registre du scrutin électronique (RSÉ).
2. Le système produit un identificateur unique pour chaque votant qui figure sur la liste.
3. Élections Ontario produit une lettre qui renferme l'identificateur unique et la distribue par la poste à chaque électeur. Cette lettre devrait être aussi sécurisée que possible**.

** En raison de contraintes de temps, il ne sera vraisemblablement pas possible de miser sur les cartes d'avis d'inscription existantes.

4. L'électeur s'inscrit en ligne en visitant un site web sécurisé dont l'adresse est fournie dans la lettre ou la carte (le site de l'inscription). L'électeur entre en communication au moyen de l'id unique fournie sur la carte et s'authentifie (établit son identité) en saisissant de l'information que l'électeur et le gouvernement sont généralement les seuls à connaître, comme :
    - la date de naissance (DDN) combinée à
    - un numéro d'id émis par le gouvernement, comme un numéro de permis de conduire (NPC) ou les quatre derniers chiffres du numéro de carte santé (NCS)†.

†Le NPC pourrait suffire pour le projet pilote; toutefois, une source d'id plus universelle devrait être utilisée dans l'avenir.

5. Si l'authentification est réussie, le système permet au votant de créer des **justificatifs d'identité de vote**, formés du même identificateur unique auquel s'ajoute un mot de passe sécurisé. Le mot de passe, qui est établi et envoyé au votant en temps réel au moment de l'inscription, pourrait être formé :
    - soit d'un mot de passe choisi par l'électeur (qui doit satisfaire aux exigences de complexité/de solidité);
    - soit d'un mot de passe aléatoire produit par le système.
6. Une fois que la période de vote est lancée, le votant exprime son suffrage à l'aide du mode de vote en réseau qu'il privilégie et s'authentifie au moyen des justificatifs d'identité établis au cours des étapes précédentes (ID de l'électeur et mot de passe personnel).
7. Si le votant choisit de voter par ordinateur, il entre dans le site web sécurisé de vote (le site de vote) avec son ID de votant unique et avec le mot de passe sécurisé créé à l'étape 5.
    I. Le votant exprime un suffrage à l'aide de l'interface en ligne.
    II. Le système supprime automatiquement le votant de la liste des votants.
8. Si le votant choisit de voter par téléphone, il compose le numéro de vote sans frais et s'authentifie en entrant son id de votant unique et le mot de passe sécurisé créé à l'étape 5.
    I. Le votant exprime un suffrage au moyen de l'interface de RVI.
    II. Le système supprime automatiquement le votant de la liste des votants.

Les neuf cas suivants sont des exceptions qui pourraient survenir pendant le flux standard décrit précédemment. Ils nécessiteraient par conséquent un traitement particulier :

1. Un votant oublie son mot de passe.
2. Un votant oublie/égare son identificateur unique.
3. Un votant déclare qu'une autre personne a utilisé ses justificatifs d'identité (usurpation d'identité).
4. Un votant désire voter en ayant recours à un mode différent.
5. De nouveaux votants sont ajoutés à la liste des électeurs une fois que les justificatifs d'identité originaux ont été envoyés (si c'est autorisé).
6. Les votants sont retirés de la liste des électeurs une fois que les justificatifs d'identité sont envoyés.
7. Trousse non reçue.
8. La trousse ne peut être lue.
9. Le votant ne possède pas l'id gouvernementale requise, ou l'authentification à l'aide de l'id gouvernementale échoue.

Le tableau qui suit donne un aperçu de la façon de traiter les exceptions au processus d'authentification et d'inscription à distance à trois stades différents du processus :

- avant le début du vote;
- pendant que le vote est ouvert, mais avant l'utilisation du justificatif d'identité;
- après l'utilisation des justificatifs d'identité pour voter.

Le traitement des exceptions proposé dans la présente section présume qu'un registre du scrutin électronique en temps réel est en place et comporte un certain degré d'intégration entre les systèmes d'Élections Ontario et le système de vote en réseau.

Avant le début du vote	**Le vote est ouvert mais le justificatif d'identité n'a pas encore été utilisé**	**Les justificatifs d'identité ont été utilisés pour voter**	
Le votant accède au site d'inscription à nouveau avec les données originales et remet à zéro le mot de passe.	Le votant accède au site d'inscription à nouveau avec les données originales et remet à zéro le mot de passe.	Aucun impact.	Mot de passé oublié
Le votant contacte le bureau d'assistance et s'authentifie (à l'aide de la DDN, du NPC, etc.)	Le votant contacte le bureau d'assistance et s'authentifie (à l'aide de la DDN, du NPC, etc.)	Traiter comme une usurpation d'identité (voir ci-après).	Identificateur oublié
Le votant se présente au bureau du directeur	Le votant se présente au bureau du directeur de		

Avant le début du vote	Le vote est ouvert mais le justificatif d'identité n'a pas encore été utilisé	Les justificatifs d'identité ont été utilisés pour voter	
de scrutin OU Le votant se fait envoyer une deuxième trousse	scrutin OU Le votant se fait envoyer une deuxième trousse		
Le votant contacte le bureau du directeur de scrutin.	Le votant contacte le bureau du directeur de scrutin.	Le votant contacte le bureau du directeur de scrutin.	Déclaration d'usurpation d'identité.
Aucun impact. Le votant peut voter au moyen de n'importe quel mode et est biffé de la liste électronique après l'avoir fait.	Aucun impact. Le votant peut voter au moyen de n'importe quel mode et est biffé de la liste électronique après l'avoir fait.	Si le registre du scrutin électronique est utilisé, il pourrait être muni d'une interface d'annulation du vote initial. Cela présume qu'identité et bulletin de vote sont liés (ce qui exige que celui-ci soit chiffré).	Le votant désire utiliser un mode différent pour voter.
De nouvelles lettres sont imprimées et envoyées automatiquement. OU De nouveaux votants doivent présenter une demande en personne comme s'ils avaient perdu leur id unique.	De nouvelles lettres sont imprimées et envoyées automatiquement. OU De nouveaux votants doivent présenter une demande en personne comme s'ils avaient perdu leur id unique.	S.O.	De nouveaux votants sont ajoutés à la liste des électeurs après l'envoi des justificatifs d'identité originaux.
Le bureau d'assistance annule leurs justificatifs d'identité pour qu'ils ne puissent voter.	Le bureau d'assistance annule leurs justificatifs d'identité pour qu'ils ne puissent voter.	Les bulletins de vote liés à ces votants sont annulés (sans que leur vie privée soit touchée).	Les votants sont retirés de la liste des électeurs une fois que les justificatifs d'identité sont envoyés.

Avant le début du vote	Le vote est ouvert mais le justificatif d'identité n'a pas encore été utilisé	Les justificatifs d'identité ont été utilisés pour voter	
Le votant appelle le bureau d'assistance, qui Envoie une nouvelle carte; ou Demande au votant de se présenter à un bureau du directeur de scrutin s'il a changé d'adresse.	Le votant appelle le bureau d'assistance, qui Envoie une nouvelle carte; ou Demande au votant de se présenter à un bureau du directeur de scrutin s'il a change d'adresse	S.O.	Trousse d'inscription non reçue.
Le votant s'inscrit en personne à un bureau du directeur de scrutin.	Le votant s'inscrit en personne à un bureau du directeur de scrutin.	S.O.	Trousse d'inscription ne peut être lue.
Le votant s'inscrit en personne à un bureau du directeur de scrutin.	Le votant s'inscrit en personne à un bureau du directeur de scrutin.	S.O.	Le votant n'a pas l'id gouvernementale requise.

Autre mode d'authentification à distance

Plutôt que d'utiliser l'ID gouvernementale pour confirmer l'identité du votant au cours de l'inscription, une deuxième trousse renfermant un deuxième NIP pourrait être employée pour s'assurer que la personne qui s'inscrit est effectivement l'électeur. Par conséquent, il existe des éléments dissuasifs additionnels au risque d'usurpation d'identité (car il est plus difficile d'intercepter deux lettres qu'une seule). Sans se servir d'un secret partagé, les votants établissent leur identité en utilisant le seul fait qu'ils résident à leur adresse postale. La sécurité globale est réduite, mais le processus est mis à la disposition de tous les électeurs.

Le processus fonctionnerait comme suit :

- Élections Ontario produit une liste des électeurs qui est importée dans le système de vote en réseau et mise à la disposition des dispositifs et du logiciel du registre du scrutin électronique (RSÉ).
- Le système produit un identificateur unique pour chaque votant qui figure sur la liste.
- Élections Ontario produit une lettre qui renferme l'identificateur unique et la distribue par la poste à chaque électeur. Cette lettre devrait être aussi sécurisée que possible**.

** En raison de pressions accrues au niveau de l'échéancier, il sera vraisemblablement impossible de miser sur les cartes d'avis d'inscription existantes.

- L'électeur s'inscrit en ligne en visitant un site web sécurisé dont l'adresse est fournie dans la lettre ou la carte (le site de l'inscription). L'électeur entre en communication au moyen de l'id unique fournie sur la carte et étaye sa déclaration d'identité en entrant sa date de naissance.

- L'électeur crée un mot de passe secret pendant le vote.
- Le système crée un deuxième numéro (un NIV) et une deuxième lettre est imprimée et postée.
- Une fois que l'électeur a reçu la deuxième lettre, il est prêt à voter en ligne (ou par téléphone).

AVANTAGES

Bien que la vérification de l'identité en utilisant deux fois la même méthode ajoute très peu à la sécurité, elle peut ajouter à la *perception* d'une sécurité accrue et par conséquent contribuer à l'atténuation du risque d'usurpation d'identité.

Toutefois, l'avantage principal d'avoir recours à un deuxième envoi postal pour doter l'électeur d'un deuxième identificateur unique consiste à permettre à Élections Ontario de mettre en œuvre un processus universellement accessible et n'exige pas que les électeurs possèdent un permis de conduire, comme l'exigerait les restrictions actuelles sur les secrets partagés disponibles. En outre, un processus qui fait effectivement suivre l'envoi postal initial d'un envoi de suivi est moins complexe sur le plan technique que l'intégration de l'authentification basée sur un système tiers ou sur des éléments de données.

INCONVÉNIENTS

L'inconvénient principal du recours à un deuxième envoi postal est qu'il accroît considérablement le temps qui doit s'écouler entre l'inscription en ligne et l'établissement des justificatifs d'identité. Dans le processus à distance standard décrit dans la sous-section précédente, il est instantané. Dans cet autre processus, le temps d'attente entre l'inscription en ligne et la réception par courrier du justificatif d'identité lié au vote final pourrait atteindre jusqu'à une semaine. Cela réduit le temps de vote potentiel d'un maximum d'une semaine et établit obligatoirement une période d'inscription du votant plus courte, car il faut fixer une date limite plus rapprochée afin de prévoir du temps pour la réception de la deuxième lettre. Les retards diminueront vraisemblablement l'adoption, en particulier pour les électeurs qui vivent dans des régions où il n'y a pas de livraison à la maison. De fait, il se peut que la carte arrive tellement tard que les électeurs disposent de peu ou de pas de temps pour voter.

Authentification supervisée

Les votants qui visitent un bureau de scrutin pour voter au moyen du mode de vote en réseau seraient authentifiés par le personnel d'élections Ontario. Un membre du personnel de scrutin vérifierait l'id physique des votants et leur admissibilité, et les autoriserait à utiliser l'appareil de vote. L'utilisation de l'id physique constitue le mode d'authentification le plus solide qui soit disponible; toutefois, il exigerait qu'un membre du personnel de scrutin mette en place une deuxième étape manuelle : autoriser le votant à utiliser l'appareil de vote.

Le flux du processus serait le suivant :

1. Élections Ontario produit une liste des électeurs et cette liste est importée dans le système de vote en réseau et mise à la disposition du registre du scrutin électronique (RSÉ).
2. Le système produit un identificateur unique pour chaque votant qui figure sur la liste.
3. Le votant arrive au bureau de scrutin avec une id physique.

4. Le secrétaire du bureau de vote vérifie l'identité du votant à la main ainsi que son admissibilité dans une liste électorale centralisée au moyen du RSÉ.
5. Si le votant préfère voter à l'aide du bulletin de vote sur papier, le secrétaire du bureau de vote biffe le votant de la liste au moyen du logiciel du RSÉ.
6. Si le votant préfère voter par ordinateur, le secrétaire du bureau de vote code une carte à puce intelligente à l'aide du RSÉ et la remet au votant. La carte à puce intelligente renferme maintenant l'identificateur unique du votant*.
    - i Le votant insère la carte à puce intelligente dans l'ordinateur de vote, qui authentifie le votant au moyen de l'id unique archivé temporairement sur la carte.
    - ii Le votant fait des sélections en se servant du bulletin de vote à l'écran.
    - iii Pour refuser le bulletin de vote ou le gaspiller intentionnellement, le votant utilise l'interface ordinateur pour sur-voter ou sous-voter.
    - iv Le votant exprime son suffrage au moyen de l'interface en ligne.
    - v Le votant est automatiquement biffé de la liste des votants dès que le bulletin de vote est déposé.

* Seul l'ordinateur de vote peut lire le contenu de la carte.

- i Si le votant préfère voter par téléphone, le secrétaire du bureau de vote utilise le logiciel RSÉ pour produire un numéro d'identification du votant (NIV) unique qui sera utilisé pour authentifier le votant au moyen du système RVI**. Il est à noter qu'il existe un système unique de vote à distance et de vote sur site, et que les identificateurs doivent être les mêmes pour tous les modes.
- ii Le secrétaire du bureau de vote imprime le NIV et remet l'imprimé au votant.

** Le NIV inclut : l'id unique du votant et un code de laisser-passer aléatoire. D'une longueur pouvant habituellement atteindre 16 chiffres.

- i Le votant saisit le NIV à l'aide du clavier téléphonique. de l'aide pourrait être fournie aux votants handicapés grâce à un appareil ou accessoire fonctionnel ou à l'assistance d'un membre du personnel de scrutin.
- ii Le votant fait des choix au moyen du menu RVI.
- iii Pour refuser le bulletin de vote ou le gaspiller intentionnellement, le votant utilise la RVI pour sur-voter ou sous-voter.
- iv Le votant exprime son suffrage au moyen de la RVI.
- v Le votant est automatiquement biffé de la liste des votants (dès que le bulletin de vote est déposé).

Les quatre cas suivants sont des exceptions qui pourraient survenir pendant le flux standard décrit précédemment et qui nécessiteraient par conséquent un traitement spécial :

Exception	Traitement
Le RSÉ montre que le votant a déjà voté.	Le directeur de scrutin décidera si le bulletin de vote précédent doit être annulé à l'aide du RSÉ et si le votant peut voter de nouveau.
La carte à puce intelligente attribuée au votant ne fonctionne pas.	Le RSÉ permet de produire une nouvelle carte. Aucun impact.
Un votant qui n'est pas dans la liste électorale désire y être ajouté et voter par le système en réseau. (permis)	Le votant est ajouté à la liste des votants à l'aide du RSÉ (par un agent de révision), mais peut voter seulement sur un bulletin sur papier. (privilégié) S'il n'y a pas de bulletins de vote sur papier : il existe des options pour ajouter des votants et délivrer de nouveaux justificatifs d'identité en temps réel.
Il n'y a pas de connexion internet. Le RSÉ ne peut être utilisé, des cartes à puce intelligentes ne peuvent être créées, des votes par ordinateur ne peuvent être déposés, et les votants ne peuvent être biffés de la liste. **Noter** que le risque que cette situation se produise peut être atténué grâce à l'utilisation de connexions internet redondantes.	Les votants ne seront pas en mesure d'utiliser le système de vote en réseau. S'il y a un bulletin de vote sur papier, les votants devraient : 1. ne pas être autorisés à voter, ou 2. déposer des bulletins de vote sur papier provisoires devant être validés plus tard, ou 3. déposer des bulletins de vote standards, qui créent un risque de bulletins de vote multiples. Dans les cas 2 et 3, le secrétaire du bureau de vote devra inscrire à la main les mises à jour au registre du scrutin et les synchroniser ultérieurement.

Recommandations principales

- Dans le cas de l'authentification à distance standard, un processus d'inscription en deux étapes avec envoi postal unique et utilisation d'un secret partagé sous forme d'une id gouvernementale est le plus sécurisé. Ce processus consisterait en l'utilisation d'une id unique produite par le système de concert avec la DDN et le NPC, ce qui occasionnerait la remise en ligne du mot de passe final pour le vote. Le recours à un deuxième envoi postal ne procurerait pas de sécurité ajoutée.
- La date de naissance d'un électeur, que nombre de personnes peuvent connaître, n'est pas suffisamment sécurisée pour authentifier un électeur pendant le processus d'inscription.
    - L'ID gouvernementale constitue par conséquent un moyen beaucoup plus solide de vérifier l'identité.

    - Bien que le permis de conduire ne constitue pas un mécanisme idéal, parce que de nombreux électeurs n'obtiennent ou ne peuvent obtenir un permis de conduire, c'est vraisemblablement la seule forme d'ID qu'Élections Ontario sera en mesure d'utiliser à des fins d'authentification dans le projet pilote.
    - Si un électeur est incapable de s'authentifier à l'aide d'un permis de conduire, il peut s'inscrire en se présentant à un bureau du directeur de scrutin.
- L'électeur doit toujours être en mesure de se présenter à un bureau du directeur de scrutin pour s'inscrire en personne si l'inscription en ligne ne fonctionne pas (par exemple, si l'électeur ne possède pas la preuve d'identité requise).
- Afin que le vote à distance par ordinateur et le vote à distance par téléphone soient possibles, l'id de l'utilisateur et le mot de passe doivent être formés de suites numériques solides.
- Les annulations et la délivrance de nouveaux justificatifs d'identité devraient exiger que les électeurs se présentent en personne à un bureau d'ÉO.
- Les nouveaux justificatifs d'identité peuvent être envoyés par SMS/courriel de la plateforme de votation afin que le personnel du bureau d'assistance ne puisse y avoir accès. Les électeurs devront donc fournir leurs coordonnées de SMS ou de courriel lorsqu'ils font une déclaration.
- Une trousse envoyée par la poste suffit pour le processus d'authentification standard à distance, car elle établit un équilibre acceptable entre la sécurité et la facilité d'utilisation pour l'électorat.

6.2 LE VOTE

La section qui suit donne un aperçu de la façon dont les quatre modes de scrutin de la liste retenue pourraient être mis en œuvre dans un modèle intégré. La faisabilité de chacun des modes sera évaluée dans les sections ultérieures.

Le vote sur site

Après avoir identifié le votant à l'aide d'une identification acceptée par la loi, le membre du personnel de scrutin validerait l'admissibilité du votant au moyen d'un registre du scrutin en ligne (s'assurer que le votant figure sur la liste électorale et n'a pas encore voté). Le membre du personnel de scrutin donne alors au votant un jeton (p. ex., une carte à puce intelligente ou un NIV sur un morceau de papier) qui permettra au votant d'utiliser l'un des appareils de vote fournis (ordinateurs ou téléphones).

Si le votant utilise un ordinateur, il s'authentifiera en insérant le jeton dans l'ordinateur de vote. Le bulletin de vote sera conçu de manière à paraître aussi clair et lisible que possible. La facilité d'interaction du votant avec le système sera le plus possible améliorée grâce à la technologie d'assistance comme les écrans tactiles, les lecteurs d'écran, les écouteurs, et d'autres appareils ou accessoires fonctionnels. Les votants seront en mesure de distinguer clairement les noms des candidats sur un bulletin de vote en ligne qui se conforme le plus possible aux exigences énoncées dans la loi électorale; toutefois, il est recommandé que le bulletin de vote puisse être disposé en ordre aléatoire des noms de candidat pour empêcher une perte possible de confidentialité causée par des empreintes digitales laissées sur les écrans tactiles.

bien que le système englobe des éléments (dialogues de confirmation, etc.) pour mieux s'assurer que les votants ne se livrent pas par erreur à un exercice insuffisant ou excessif de leur droit de vote, il permettra aux votants de déposer intentionnellement des bulletins de vote gaspillés ou invalides s'ils décident de le faire.

Si le vote a lieu par téléphone, le votant s'authentifie en tapant le NIV fourni par le membre du personnel de scrutin sur le bulletin de vote à l'aide du clavier à douze chiffres du téléphone. Le bulletin de vote prendra la forme de directives sonores claires et faciles à comprendre. Le votant pourra contrôler la vitesse et le volume de lecture des directives et les options du menu de vote et recevoir des confirmations claires des choix.

VOTE À DISTANCE

Le fait de voter à distance repose sur les mêmes interfaces informatiques et téléphoniques que pour le vote sur site, sauf que les votants doivent s'authentifier en tapant leur id d'électeur et le mot de passe numérique qu'ils ont obtenu pendant le processus d'inscription. Le système du menu téléphonique et l'interface du bulletin de vote en ligne demeureront les mêmes.

ACCUSÉS DE RÉCEPTION

Le système doit fournir aux votants un accusé de réception une fois qu'ils ont exprimé leur suffrage. Cet accusé de réception leur permettra de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de dépouillement. Pour éviter de donner prise à la contrainte ou à la corruption, l'accusé de réception ne renfermera pas de renseignements lisibles portant sur le choix du votant. En outre, l'accusé de réception ne doit permettre à personne d'avoir accès au système pour relier les votants au bulletin de vote qu'ils ont déposé.

Le registre du scrutin électronique (RSÉ)

Si le vote en réseau à distance a lieu parallèlement au vote en réseau sur site, un registre du scrutin électronique sera nécessaire pour gérer la liste des électeurs et empêcher que le même votant vote plusieurs fois. dans ce scénario, les membres du personnel de scrutin d'Élections Ontario pourraient avoir recours au système de gestion des élections (SGE) pour gérer la liste des électeurs en temps réel au cours de l'événement, notamment en biffant des votants, en ajoutant et en supprimant des électeurs, en actualisant des fichiers, et en enregistrant des jetons en vue de l'accès aux terminaux de votation.

Les bureaux de vote devraient être munis d'ordinateurs donnant accès au registre du scrutin électronique et prendre en charge le vote en réseau et le vote sur bulletin de papier sur site. Cela nécessiterait des interactions entre le SGE et le système de vote en réseau (SVR) que procurerait un fournisseur.

Le processus qui suit décrit les interfaces qui devraient exister entre le SGE et le SVR au cours des trois étapes principales de l'événement (avant, pendant et après le vote). Les données transférées entre le SGE et le SVR devraient idéalement être établies à l'aide des services web.

AVANT LE DÉBUT DU SCRUTIN

1. Le SGE fournit au système de vote une liste des votants initiale (p. ex. 100 000 noms).
2. Le SVR produit au préalable 120 000 justificatifs d'identité des votants (NIV/mots de passe). Les 20 000 supplémentaires sont conservés en réserve pour le traitement d'ajouts, d'annulations, de remises à zéro, etc.
3. Pour gérer le code d'utilisateur envoyé aux votants par la poste :
    a. Le SGE identifie les électeurs qui reçoivent une trousse d'inscription au vote en réseau avec une id de VR et transmet ces données au SVR par une interface.
    b. Le SGE gère le processus de transmission des cartes.
4. Le SVR envoie les données au SGE pour déterminer quels électeurs établissent un mot de passe en ligne au moyen de l'interface web du SVR.

PENDANT LA PÉRIODE DE VOTE

5. Comme les changements à la liste des votants sont gérés par le SGE, les changements qui affectent le vote en réseau doivent être synchronisés avec le SVR* :
    a. Les électeurs qui sont retirés du système (si le votant a déjà exprimé son suffrage par voie électronique, le bulletin de vote chiffré pourrait être identifié et marqué invalide).
    b. Les électeurs qui passent d'une cé à une autre et qui votent par conséquent sur un bulletin de vote différent. (le bulletin de vote chiffré pourrait être identifié et marqué invalide.)
    c. Ajout de nouveaux votants : un justificatif d'identité supplémentaire est attribué à ce nouveau votant.
6. La liste des électeurs dans le SGE est actualisée à l'aide des données du SVR qui indiquent si un cybervotant a voté*.
7. Le SGE doit également être en mesure de demander au SVR d'annuler un vote électronique (lié à un votant)*.
8. Le membre du personnel de scrutin utilise le SGE pour coder un jeton qui autorise le votant à se servir de l'ordinateur de vote, puis l'interface doit prendre ce geste en charge, et une autre communication doit être établie avec le SVR, qui fournit les données devant être incluses dans le jeton en vue de l'authentification du votant.

APRÈS LA PÉRIODE DE VOTE

9. Le SVR transmet la liste finale des cybervotants au SGE.
10. Ce pourrait être fait par transfert de fichier plutôt que par service web.

*Des changements sont exigés au SGE pour permettre aux membres du personnel de scrutin de poser ces gestes.

Fonctionner en l'absence du registre du scrutin électronique

Si seul le vote à distance est mis en œuvre parallèlement au mode de scrutin conventionnel, et si les modes de scrutin en réseau sur site ne sont pas utilisés, un registre du scrutin électronique n'est pas nécessaire à proprement parler. La fonction principale du registre du scrutin électronique consiste à contrôler le nombre de bulletins de vote déposés par un utilisateur dans plusieurs modes de scrutin tout en conférant un caractère dynamique à la liste des votants en permettant des ajouts et des suppressions au cours du processus de vote. Si le vote en réseau est mené seulement au moyen des modes à distance, et si la liste des votants demeure statique pendant la période de vote, un registre du scrutin électronique n'est pas nécessaire.

Dans un scénario qui utilise seulement le vote en réseau à distance combiné aux bulletins de vote sur papier, un registre du scrutin en ligne n'est pas nécessaire à proprement parler, pourvu qu'un autre mode puisse être mis en œuvre pour empêcher les votants de voter en ligne, puis de voter sur un bulletin sur papier, ou l'inverse. Chaque mode (réseau et papier) gérera effectivement sa propre liste en parallèle et les besoins de synchronisation seront pris en charge manuellement à titre d'exceptions et ne seront pas traités en temps réel.

- le SGLE ou le SGE fournira la liste des votants finale versée au dossier et produira les listes sur papier qui sont utilisées dans les bureaux de scrutin.
- Le SGLE ou le SGE fournira également au système de vote en réseau la liste des votants préliminaire (LVP). Le système de vote en réseau attribuera ensuite un identificateur unique à chaque électeur (l'id d'électeur).
- Les électeurs qui désirent voter à distance s'inscriront en ligne ou par téléphone et associeront d'autres justificatifs d'identité à leur id d'électeur.
- L'inscription du votant doit prendre fin avant la date du vote par anticipation afin que les listes imprimées puissent être produites et distribuées.
- Les électeurs qui s'inscrivent aux modes de scrutin en réseau à distance seront cantonnés dans le vote en réseau et ne pourraient voter sur un bulletin en papier. (*Des exceptions sont possibles dans le cas des électeurs désireux de demander l'annulation de leurs justificatifs d'identité de VR pour qu'ils puissent voter sur un bulletin de papier).
- La liste des votants se trouvant dans des bureaux de scrutin ne sera pas synchronisée automatiquement avec la liste de vote en réseau en ligne.

La liste électorale électronique du système de vote en réseau renferme la liste des votants en temps réel qui sont autorisés à voter au moyen des modes de scrutin en réseau. Elle fonctionne indépendamment de la liste des votants d'ÉO et est conçue de manière à offrir a) la radiation en temps réel des personnes qui votent en réseau; et b) le lien des votants avec les bulletins de vote chiffrés. Elle n'est pas facultative et sera comprise dans le produit de vote en réseau.

Si le fait de cantonner les votants dans le mode de vote en réseau limite le choix de l'électeur de façon inacceptable, la liste du SGLE/SGE pourrait être synchronisée régulièrement (chaque jour) avec le système en ligne en examinant la liste des radiations sur papier et en les biffant en mode électronique de la liste du vote en réseau. Toutefois, cette mesure mettrait directement en péril le principe « un votant, un vote ».

Les votes en réseau déposés par des votants ayant également exprimé leur suffrage en personne sur un bulletin de vote sur papier pourraient aussi être retirés quotidiennement, ou encore après l'élection; toutefois, ce geste laisserait à penser que le vote multiple est possible d'une certaine manière, et que le principe « un votant, un vote » n'est pas étayé.

Le vote sur site, mené seulement au moyen du mode traditionnel du bulletin de vote sur papier, fonctionnerait comme suit :

1. La liste imprimée est distribuée aux bureaux de scrutin et indique les votants qui se sont inscrits pour voter à distance.
2. Le votant présente son id au bureau de scrutin et le membre du personnel de scrutin vérifie son admissibilité sur la liste imprimée.
3. Le membre du personnel de scrutin donnera un bulletin de vote seulement aux votants qui ne sont pas inscrits pour voter en ligne.
4. Le membre du personnel de scrutin biffe le votant de la liste sur papier.

Le vote en réseau, qui ne serait disponible que par les modes à distance, fonctionnerait comme suit :

1. Le votant s'inscrit pour voter à distance (au moyen d'un téléphone ou d'un ordinateur) avant le début de la période de vote par anticipation.
2. Le votant s'authentifie en ligne au moyen de l'id d'électeur et du mot de passe.
3. Le système de vote en réseau traite le vote et biffe le votant.
4. Le votant n'est pas en mesure de voter une deuxième fois en utilisant l'un ou l'autre des modes à distance.

En l'absence d'un lien fonctionnel entre la liste des électeurs archivée et gérée par le système de vote en réseau et la liste des votants d'élections Ontario, les révisions seraient traitées comme suit :

1. Les membres du personnel d'ÉO corrigent et actualisent la liste des votants au moyen des systèmes et processus finaux actuels.
2. Les mises à jour sont synchronisées au besoin avec le système de vote en réseau à l'aide de processus manuels.
3. Une synchronisation finale est effectuée entre le système de vote en réseau et le SGLE/SGE après l'événement.

Les votants pourraient s'inscrire pour voter en réseau, puis décider de ne pas le faire ou être empêchés de le faire. S'ils demeurent cantonnés, ils pourraient ne pas être en mesure de voter du tout. Les électeurs qui se sont inscrits au vote en réseau mais qui n'ont pas voté de cette façon d'ici la fin de la période de vote en réseau pourraient se faire annuler leurs justificatifs d'identité de sorte qu'ils pourraient quand même voter sur papier le jour du scrutin.

Les ajouts à la liste rendraient le processus plus complexe et nécessiteraient plus de temps :

- L'ajout d'un nom nécessiterait l'envoi postal de cartes d'id d'électeur, la synchronisation avec le système de vote en réseau, et l'ajout de mécanismes de suivi de cartes supplémentaires.
- Les votants qui doivent être supprimés de la liste une fois qu'elle est dans le système en ligne peuvent être retirés manuellement au moyen d'une interface administrative.

Recommandations principales

- Si le vote en réseau sur site est offert, la fonctionnalité du registre du scrutin électronique doit être mise en œuvre, y compris une interface en temps réel pour les membres du personnel de scrutin.
- Si seul le vote en réseau à distance est offert et que le registre du scrutin électronique est éliminé, la liste des votants en réseau devrait demeurer statique durant la période de vote. Autrement dit, les votants en réseau seront en général cantonnés.
- Utiliser deux systèmes d'autorisation distincts pour le vote sur site : un pour le vote par ordinateur basé sur une carte à puce intelligente et un autre pour le vote par téléphone basé sur un NIV imprimé. Le principe qui sous-tend cette recommandation est l'utilisation d'un système davantage utilisable (carte à puce intelligente) lorsque c'est possible et la limitation de l'usage des NIV, qui présentent des difficultés au niveau de la facilité d'utilisation et de l'accessibilité.
- Si un votant se présente sur un site et qu'il est indiqué qu'il a déjà voté, le directeur de scrutin statuera sur la question de la supposition de personne du votant.
- Le système devrait permettre aux votants de refuser des bulletins de vote en offrant une option « refuser le bulletin de vote » ou « aucune des options qui précèdent », en plus de permettre l'exercice insuffisant ou excessif du droit de vote.
- Les écrans tactiles, qui sont recommandés en raison de leur facilité d'utilisation et de leur accessibilité, pourraient révéler des empreintes digitales et par conséquent les choix de vote populaires si l'ordre des candidats est statique conformément à la réglementation (paragraphe 34(2) de la *loi électorale*). Pour atténuer ce risque possible pour la confidentialité, Élections Ontario devrait demander une exception au paragraphe 34(2) et mettre en œuvre l'ordre aléatoire des noms des candidats pour le bulletin de vote en ligne.

6.3 ARCHIVAGE DES VOTES

Le chiffrement a lieu dans l'ordinateur du votant ou dans les serveurs de l'élection en cas de vote par téléphone.

Une fois que le votant a déposé son bulletin de vote par ordinateur ou par téléphone, il est archivé dans l'« urne électronique » du système de vote en réseau, où il demeure chiffré pour un secret absolu. Le système sera maintenant responsable de préserver la sécurité et l'intégrité des données de vote qu'il archive jusqu'au début du processus de déchiffrement et d'établissement des résultats.

Pendant l'élection, les mesures de sécurité visant le vote en réseau (systèmes de détection des intrusions, fichiers journaux des activités, etc.) détecteront toute tentative d'utilisateurs externes ou internes de supprimer des votes de l'urne ou d'ajouter des votes contrefaits. Le système mettra en œuvre des mesures de sécurité pour empêcher de mettre en péril la confidentialité du votant, la publication interdite de résultats intermédiaires, le remplissage de bulletins de vote, ou la modification et la suppression de votes.

6.4 COMPILATION

Le système de vote se fermera automatiquement au moment indiqué par Élections Ontario : les votants ne pourront entrer dans le système, mais ceux qui sont en train de voter auront un certain temps pour terminer.

Seuls les membres du conseil de gestion du vote en réseau peuvent lancer le processus de déchiffrement. Une majorité préétablie de membres du conseil de gestion du vote en réseau se réunira pour établir la clé de déchiffrement de l'élection, qui n'est pas disponible au cours du processus de vote.

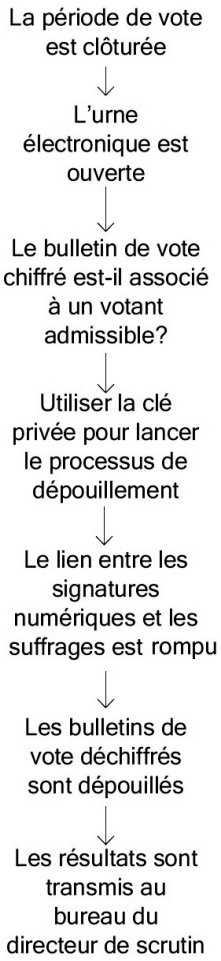
Idéalement, l'urne est déplacée dans un environnement sécurisé et isolé dans les locaux d'Élections Ontario qui ne sont pas branchés à internet ni à aucun autre réseau de communication.

Le système vérifiera que tous les votes contenus dans les urnes sont déposés par des votants admissibles. Il empêchera également le déchiffrement des votes multiples par le même votant, dont la prévention du dénombrement de votes qualifiés d'invalides par un utilisateur autorisé (comme dans les cas de déclaration d'usurpation d'identité).

Il sera impossible d'établir une corrélation entre l'ordre des bulletins de vote déchiffrés et l'ordre de leur dépôt, et par conséquent d'établir un lien entre les bulletins de vote déchiffrés et les votants en utilisant un processus de mélange.

Cette tâche terminée, le conseil de gestion du vote en réseau certifiera la liste des bulletins de vote déchiffrés et préparera un rapport, faisant notamment état de tous les bulletins de vote valides et invalides pour chaque candidat, par circonscription électorale.

Les résultats seront rapportés au directeur de scrutin de chaque circonscription électorale et ajoutés au système de regroupement des résultats géré par élections Ontario.



6.5 VÉRIFICATION

Le système permettra aux vérificateurs indépendants de vérifier et de certifier l'intégrité et l'authenticité des composantes du système utilisées dans le traitement des urnes électroniques, y compris l'authenticité des logiciels, l'intégrité du système, l'intégrité et l'authenticité des fichiers journaux générés, etc. Les vérificateurs pourront vérifier que les votes dans l'urne sont ceux de votants admissibles à n'importe quel moment au cours de l'élection.

Ainsi, des vérificateurs indépendants ou le conseil de gestion du vote en réseau pourront procéder à des recomptages parallèles à partir de la liste certifiée des bulletins de vote déchiffrés ou de nouveaux processus de déchiffrement et de compilation si nécessaire. Les vérificateurs doivent être en mesure de travailler à partir des bulletins de vote déchiffrés et d'obtenir des résultats traduits en clair susceptibles d'être comparés à ceux qui sont générés par le système.

7. ANALYSE DES SCÉNARIOS RETENUS

Une recherche exhaustive sur les options de vote en réseau a permis d'éliminer six des dix options, ce qui laisse quatre options à étudier davantage. Le chapitre précédent constituait une revue de la façon dont chacun de ces scénarios cadrerait dans le processus de vote. Le présent chapitre analyse comment les quatre scénarios qui restent cadrent dans le contexte actuel documenté dans le chapitre 4, analyse le soutien à la liste retenue des principes de vote en réseau documenté du chapitre 5, et expose une analyse complète des facteurs de risque et de sécurité.

ÉVALUER LA PERTINENCE POUR LE PROJET PILOTE

Le processus de recherche sur le vote en réseau s'est traduit par une liste des quatre scénarios retenus de vote en réseau qui nécessitaient une analyse plus approfondie. La présente étude de cas conclut que la combinaison de ces quatre scénarios en un modèle unique pourrait étayer les principes retenus et pourrait largement fonctionner à l'intérieur des contraintes et dans le respect des objectifs du projet pilote. Ces quatre modes sont :

1. Vote sur site, par ordinateur, avec authentification supervisée;
2. Vote sur site, par téléphone, avec authentification supervisée;
3. Vote à distance, par ordinateur, reposant sur une authentification par mot de passe;
4. Vote à distance, par téléphone, reposant sur une authentification par mot de passe.

ORGANISATION DE LA PRÉSENTE SECTION

Dans les sections qui suivent, ce modèle intégré sera évalué à la lumière :

- d'une analyse contextuelle reposant sur les contraintes définies au chapitre 2;
- d'une analyse fondée sur les principes fondamentaux du vote en réseau définis au chapitre 3;
- d'un survol des risques sur le plan de la sécurité, des opérations et du votant auxquels chaque scénario serait confronté.

7.1 ANALYSE CONTEXTUELLE

La liste des quatre scénarios retenus qui sont décrits s'inscrit dans les facteurs contextuels définis au chapitre 2 à des degrés divers. La section qui suit renferme une analyse de la mesure dans laquelle chaque scénario cadre dans l'orientation stratégique d'élections Ontario, fonctionne dans les contraintes connues, répond aux besoins du public cible, et étaye les principes de vote définis.

Analyse fondée sur l'orientation stratégique

ÉLARGIR LES OPTIONS DE VOTE

La réalisation d'un projet pilote sur le vote par téléphone et par ordinateur, soit les modes les plus répandus de vote sous forme électronique, s'harmonise avec la stratégie d'Élections Ontario qui consiste à innover et à établir de nouveaux repères. En outre, le fait de proposer de nouveaux modes de scrutin en réseau s'inscrit bien dans l'intention stratégique d'Élections Ontario de donner à l'électorat plus de choix, d'accroître les possibilités de voter, et d'appuyer l'accessibilité globale au processus.

Toutefois, l'analyse n'appuie pas la conclusion que le fait d'offrir des modes de vote sur site élargira beaucoup l'éventail des choix. Bien que les électeurs ayant de la difficulté à se présenter dans un bureau de scrutin accueilleront avec joie l'option de voter de la maison ou du travail, le vote sur site procurerait une option de plus uniquement aux votants qui désirent exprimer un suffrage par voie électronique, mais qui n'ont pas accès facilement à internet ou à un téléphone. Prévoir des locaux de vote en réseau accessibles ajouterait un choix, mais cet avantage serait négligeable, notamment dans le contexte d'un projet pilote.

Analyse fondée sur les contraintes

APPUYER L'ACCÈS UNIVERSEL

Bien que l'échéancier soit serré, il est possible d'acquérir, de personnaliser et de déployer un système de vote en réseau disponible sur le marché (COTS) pouvant être utilisé au cours d'une élection partielle d'ici le premier trimestre de 2012. Un système qui combine des modes de vote par ordinateur et par téléphone, comme le recommande le présent document, pourra offrir un processus et une interface commodes à un grand nombre de votants.

Les modes de scrutin à distance peuvent comprendre une interface web très accessible qui est à la fois utilisable et compatible avec la technologie d'aide au vote, à la condition que les normes correctes soient appliquées et que l'expérience de l'utilisateur soit à la fois bien conçue et bien mise à l'essai.

RÉPONSE AUX PRÉOCCUPATIONS DU PUBLIC PAR LA SÉCURITÉ ET LA TRANSPARENCE

Bien que la portée d'internet soit vaste tant sur le plan géographique que du point de vue démographique, l'ajout d'un mode de scrutin par téléphone fait en sorte que le vote à distance est aussi accessible que possible. Les électeurs qui n'ont pas accès à internet pourront quand même voter en se servant du téléphone. Le fait d'offrir des options de vote sur site permettrait d'augmenter le nombre d'options disponibles et de s'assurer qu'une expérience accessible et étayée est disponible, mais le déploiement d'un tel mode de scrutin n'est pas nécessaire pour donner une accessibilité importante aux votants.

Il serait possible de répondre aux préoccupations du public et des médias au sujet de problèmes éventuels de sécurité, de confidentialité et d'intégrité liés au vote sous forme électronique en acquérant un système offrant les meilleures solutions disponibles au niveau de la sécurité. Des résultats de vérification indépendants et publiés seront cruciaux pour répondre à ces préoccupations valides et les apaiser.

FONCTIONNER EN RESPECTANT LES CONTRAINTES LIÉES AU PROCESSUS

En plus d'apaiser les préoccupations par des moyens techniques, il est possible de s'occuper de la perception au moyen d'une campagne publique exhaustive et efficace de communications qui reconnaît la validité des préoccupations et illustre la manière de s'en occuper.

Le vote à distance par téléphone et par ordinateur cadre bien avec le processus et les contraintes opérationnelles relevés par élections Ontario. Ces modes de scrutin peuvent être adaptés facilement pour être utilisés pendant le vote par anticipation, et non le jour du scrutin lui-même. de fait, l'élimination du vote électronique le jour du scrutin présente l'avantage de faire diminuer le risque de collisions entre les votants en ligne et les votants utilisant un bulletin de vote sur papier et élimine le risque qu'un électeur ne puisse voter parce qu'il ne s'est pas inscrit à l'avance.

DÉFIS CONCERNANT LES CONTRAINTES EXISTANTES AU NIVEAU DU PERSONNEL ET DU SYSTÈME

Toutefois, les modes de scrutin sur site présentent un défi opérationnel plus difficile à relever, car ils augmenteraient le niveau de complexité pour Élections Ontario et nécessiteraient un changement organisationnel. Plus précisément, le déroulement en parallèle du vote à distance et du vote sur site exigerait la mise en œuvre d'une liste des votants électronique en temps réel (registre du scrutin) pour contrôler le nombre de bulletins de vote déposés par un votant un jour donné.

MODES DE SCRUTIN SUR SITE IMPOSERONT DES CONTRAINTES À LA CAPACITÉ DE CHANGEMENT

Le déploiement d'un système de registre du scrutin électronique nécessiterait des changements aux systèmes existants de la liste des votants finale d'Élections Ontario ainsi qu'une formation et des mesures de logistique additionnelles au niveau des bureaux de scrutin, notamment la nécessité de distribuer le matériel et le logiciel du registre du scrutin et d'en assurer le soutien. Comme seuls les modes de scrutin à distance sont en jeu, les besoins rattachés au registre du scrutin en temps réel sont réduits.

De même, la mise en œuvre du vote sur site fera augmenter les dépenses, car il faudra acquérir, distribuer, soutenir et gérer le matériel de scrutin et du registre du scrutin. Le déploiement limité aux modes de scrutin à distance éliminera ces dépenses et améliorera la variabilité des coûts.

Le déploiement restreint aux modes de scrutin à distance est la stratégie qui cadrerait le mieux avec la capacité de changement actuelle d'élections Ontario, tout en permettant de réaliser ses objectifs stratégiques et ceux d'un projet pilote. Compte tenu des risques liés à un échéancier très serré (période de déploiement du projet d'environ six mois), il est recommandé d'acquérir un système disponible sur le marché (COTS) auprès d'un fournisseur reconnu.

Analyse fondée sur le public cible et les parties prenantes

Les parties prenantes consultées ont fait écho à la stratégie déclarée d'Élections Ontario en mettant en relief le besoin d'offrir des options et d'accroître le degré de commodité pour les électeurs. Leurs préoccupations laissent entrevoir qu'une solution mettant l'accent sur la sécurité, la confidentialité et l'indépendance est nécessaire.

JOINDRE LE PLUS GRAND NOMBRE D'ÉLECTEURS POSSIBLE

Bien qu'une très grande majorité de la population ontarienne a accès à internet (80 % s'en servent chaque jour) et que le téléphone est presque universel (99 %), il importe que la solution soit très accessible. En offrant des modes de scrutin en réseau en plus du bulletin de vote sur papier actuel, un modèle unifié à quatre modes permettrait de joindre le plus grand nombre possible d'ontariens grâce à tout un éventail d'options de vote. Le vote sur site par ordinateur offrirait une option accessible aux personnes qui ont de la difficulté avec le bulletin de vote sur papier, mais qui n'ont pas internet à la maison. Le vote par téléphone donnerait une option aux personnes ayant de la difficulté à se présenter en personne, mais qui n'ont pas accès à internet.

7.2 ANALYSE BASÉE SUR LES PRINCIPES

Les quatre scénarios doivent également être évalués quant au soutien qu'ils apportent aux huit principes clés dont Élections Ontario se sert pour orienter le projet de vote en réseau.

PRINCIPE	ANALYSE
Accessibilité	Les quatre modes sont accessibles à des degrés divers. Bien que le vote par téléphone présente des problèmes de facilité d'utilisation et d'accessibilité à certains utilisateurs, c'est également la technologie la plus universellement disponible. Les problèmes d'accessibilité du vote par téléphone, notamment en ce qui a trait à la difficulté d'obtenir une autorisation sur site pour les votants qui ont un handicap visuel seraient surmontés en rendant simultanément accessible un mode de vote par ordinateur. **Technologie accessible** La mise en œuvre d'une stratégie de technologie d'aide au vote peut améliorer de beaucoup l'accessibilité du mode de scrutin par ordinateur. Par exemple, en rendant l'interface web compatible non seulement aux spécifications des DACW mais également à la technologie de lecture d'écran, les votants qui utilisent ce genre de technologie en tireront un avantage pratique. de plus, en mettant l'accent sur les nouvelles solutions basées sur des lecteurs d'écran, en général très peu coûteuses, voire gratuites, la stratégie peut faire diminuer les coûts de mise en œuvre et alléger les obstacles pour les nouveaux adoptants. **Processus d'inscription** Le plus gros problème d'accessibilité auquel les scénarios de la liste retenue sont confrontés est lié au processus d'inscription. Pour confirmer l'identité de l'électeur au cours de l'inscription aux modes de scrutin en réseau, il faudra disposer d'une pièce d'identité du gouvernement. toutefois, Élections Ontario n'a accès qu'aux numéros de permis de conduire. Ce type d'identification n'est pas universel, en particulier chez les électeurs ayant certains handicaps. Le modèle recommande que les électeurs qui sont incapables de fournir un numéro de permis de conduire pendant l'inscription doivent se présenter à un bureau du directeur de scrutin pour s'inscrire. Cette façon de faire a pour effet de créer un obstacle au niveau de

PRINCIPE	ANALYSE
	l'accessibilité pour les électeurs qui n'ont pas de permis de conduire, dont bon nombre ont peut-être des handicaps qui rendent déjà leurs déplacements difficiles. Plutôt que d'appliquer une méthode d'authentification qui dissuade les électeurs sans permis de conduire de participer, Élections Ontario pourrait privilégier une approche moins sécurisée, mais qui répond aux besoins d'une plus grande tranche de l'électorat. Le recours à un processus d'inscription fondé sur deux envois postaux séquentiels, même s'il n'est pas aussi bien sécurisé sur le plan technique (si le premier envoi postal peut être intercepté, le deuxième pourrait l'être également), s'est révélé réussi lors des élections municipales, notamment celles de Markham en 2010. L'objectif final de l'authentification est la capacité d'intégration à des fournisseurs d'authentification tiers commes serviceOntario (voir le scénario 9 concernant les avantages de cette approche). **Autres problèmes d'authentification : le vote sur site** L'impression d'un NIV, qui constitue la meilleure option pour autoriser les votants à avoir recours au scénario de vote sur site par téléphone, présente un certain nombre d'inconvénients, dont la mise en péril de l'accessibilité. Les votants ayant un handicap visuel auraient besoin d'aide pour lire le NIV imprimé. Cela présente également un problème au niveau de la confidentialité du votant (voir ci-après). Cependant, l'option d'authentification pour le vote sur site par ordinateur ne réduit pas du tout l'accessibilité au même degré.
Un votant, un vote	Si les modes de scrutin sur site et à distance étaient déployés, une liste électorale électronique centrale qui serait intégrée en temps réel au système de vote serait nécessaire afin de veiller à ce qu'un seul vote par votant soit compté. de plus, le processus de remise du NIV doit être conçu et mis à l'essai pour s'assurer qu'un seul NIV est remis à chaque votant. Si seuls les modes de scrutin à distance étaient mis en œuvre, la liste des électeurs pourrait être gérée sans registre du scrutin électronique. Comme le système de vote en réseau en ligne ne sera pas synchronisé à la liste des électeurs finale (SGLE/SGE), la mise à jour de la liste des électeurs devrait être faite autrement : En effectuant un gel de la liste en ligne basé sur la liste des votants préliminaire (LVP). Il s'agit d'une mesure raisonnable à prendre en situation de projet pilote, car le volume de révisions sera vraisemblablement bas (<5 % du total des noms). ou En actualisant la liste en ligne manuellement, au fur et à mesure des révisions (p. ex. En utilisant une interface SVR ou en téléchargeant des fichiers de données). En l'absence d'un registre du scrutin électronique, le risque serait élevé que les votants votent deux fois (une fois à distance, l'autre fois sur site) si les votants n'étaient pas cantonnés dans le mode de leur choix. quoique ce risque soit présent dans le cas du vote par anticipation sur bulletin de papier, il aurait été beaucoup plus grand dans le cas du vote en réseau et devrait être géré de manière plus dynamique.

PRINCIPE	ANALYSE
Authentification et autorisation du votant	Le mécanisme d'authentification du mot de passe qui est utilisé dans le cas du vote à distance par ordinateur et par téléphone peut constituer une façon très sécurisée d'établir l'identité du votant. En ce sens, le processus de remise de l'ID d'électeur et le mécanisme d'inscription devraient être fiables et sécurisés et des exigences strictes relatives à la longueur et à la complexité du code devraient être appliquées. De plus, les données d'identifica-tion requises pour étayer la déclaration d'identité d'un électeur durant l'inscription doivent être aussi sécurisées et solides que possible. Les renseignements personnels pouvant être aisément trouvés (date de naissance, adresse, numéro de téléphone, etc.) ne sont pas assez sécurisés, car ils rendent l'usurpation d'identité trop facile. Un acteur malveillant qui a intercepté la CAE d'un électeur et avait accès à ce type de données pourrait s'enregistrer comme votant, puis voler son vote. Une identification émise par le gouvernement (NAS, numéro de carte santé) est plus convenable et présente l'avantage d'être détenue par l'ensemble de l'électorat. Comme Élections Ontario n'aura pas accès à ces données pour le projet pilote, les numéros de permis de conduire (qui peuvent être obtenus par ÉO) constituent une solution à court terme acceptable. L'inconvénient principal est l'impact sur les électeurs qui ne détiennent ou ne peuvent détenir de permis de conduire (voir accessibilité, précédemment). C'est la combinaison de ces types de données qui réduit la probabilité d'usurpation d'identité d'un citoyen. En utilisant l'ID physique à des fins d'authentification lorsque c'est possible (sur site), le modèle à quatre modes inclut le recours au meilleur mécanisme d'identification et d'autorisation possible pour le vote en réseau. Il est difficile de prévoir quel pourcentage des votes en réseau sera exprimé à distance et sur site, mais le projet pilote donnera à Élections Ontario l'occasion d'évaluer les deux. Une fois que l'identité du votant a été établie, un registre du scrutin électronique sera un moyen très fiable de vérifier l'admissibilité de l'électeur, car il permettra aux membres du personnel de scrutin et au système de vote en réseau d'évaluer l'admissibilité en temps réel.
Prise en compte des suffrages exprimés par des votants admissibles uniquement	Les serveurs et la liste des électeurs doivent être bien protégés pour s'assurer que les votes ne peuvent être déposés par quiconque n'est pas un votant admissible.
Vérifiabilité au cas par cas	L'interface en ligne et par téléphone (RVI) peut être conçue pour doter les votants d'un moyen de confirmer leurs choix avant de déposer leur bulletin de vote. dans le cas des modes de scrutin par ordinateur, le système peut produire un accusé de réception imprimable pour doter le votant d'une vérifiabilité maximale.
Confidentialité	Le chiffrement de bout en bout qui s'inscrit dans l'approche recommandée assure la confidentialité du votant lorsqu'il utilise des ordinateurs. dans le cas du vote par téléphone, des procédures et des mesures spécifiques

PRINCIPE	ANALYSE
	doivent être instaurées*. *Le vote par téléphone présente des risques de confidentialité spécifiques qui doivent être atténués. En ce qui concerne les modes de scrutin sur site, l'emplacement physique et la conception des bornes interactives sont essentiels pour garantir que les votants puissent déposer leurs bulletins de vote de façon privée et indépendante. L'impression d'un NIV, qui constitue la meilleure option réalisable pour autoriser les votants à avoir recours à l'option de téléphone sur site, présente un certain nombre d'inconvénients, notamment en mettant en péril l'accessibilité. Les votants qui ont un handicap visuel et qui auraient besoin d'aide pour lire le NIV imprimé, seraient en situation de violation de leur confidentialité. En outre, leur capacité de voter de façon indépendante serait affectée. toutefois, l'option d'authentification pour le vote sur site par ordinateur ne réduit pas la confidentialité du votant.
Validation des résultats	La validation des résultats repose sur l'efficacité des mesures de sécurité de bout en bout et sur la tenue d'un journal et la vérification de système vigoureuses indiquées dans les exigences.
Disponibilité du service	Bien que l'impact sur le nombre de votes touchés puisse être relativement élevé en situation de panne dans un bureau de scrutin, le risque et l'impact diminuent de façon spectaculaire dans les modes de scrutin à distance. La meilleure protection contre les pannes de services passe par le genre d'infrastructure d'accueil et de matériel vigoureuse que recommande la présente étude de cas : Un centre de données fiable et sécurisé; Une connectivité internet fiable et redondante dans les bureaux de scrutin; Un processus de soutien et de remplacement de matériel qui répond aux besoins.

7.3 LES RISQUES

Bien que cette analyse laisse croire que ces quatre scénarios peuvent bien répondre aux besoins de l'Ontario, ils présentent quand même un ensemble de risques, qui sont regroupés dans les catégories suivantes :

- les risques en matière de sécurité;
- les risques liés aux opérations;
- les risques pour le votant.

Ces risques sont décrits brièvement ci-après et sont évalués en détails dans le chapitre 9, évaluation du risque.

Risques en matière de sécurité

Les risques en matière de sécurité qui doivent être gérés et atténués peuvent être subdivisés en quatre catégories, qui correspondent directement avec la liste des principes :

- vie privée et confidentialité du votant;
- intégrité du vote et exactitude des résultats;
- disponibilité du système électoral;
- vérifiabilité.

Risques liés aux opérations

Il existe une série de risques liés aux opérations qui sont associés aux scénarios de la liste retenue; ces risques peuvent être organisés suivant les quatre secteurs d'opération suivants :

- les bureaux de vote
- le centre de données
- le bureau central d'élections Ontario
- le bureau d'assistance qui soutient l'initiative du vote en réseau.

Risques pour le votant

Il existe deux catégories de risques liés aux votants : les résultats de leur interaction avec le système de vote en réseau à divers stades; et leurs perceptions du système et du vote en réseau en général.

7.4 OBJECTIFS EN MATIÈRE DE SÉCURITÉ

Pour pouvoir atténuer efficacement le risque, il importe d'établir quels sont les objectifs en matière de sécurité qui devraient être pris en compte lors du déploiement de la plateforme de vote en réseau. Les objectifs en matière de sécurité sur lesquels il conviendrait d'insister dans le cadre du projet pilote sont les suivants :

1. **Authenticité du votant** : les objectifs en matière de sécurité associés à l'authentification des votants admissibles.
2. **Secret du votant** : les objectifs protégeant la vie privée du votant.
3. **Contrôle de l'accès au système** : les objectifs liés aux méthodes d'identification et d'authentification mises en œuvre dans la plateforme de vote.
4. **Intégrité de l'élection** : les objectifs qui garantissent la cohérence et l'exactitude des bulletins de vote déposés.
5. **Disponibilité du service** : les exigences liées à la disponibilité du système électoral et à son information durant le processus électoral.
6. **Protection du service** : les objectifs associés à la protection du système électoral.
7. **Vérification et comptabilité ouvertes** : les objectifs qui assureront une vérifiabilité exacte du système électoral et la traçabilité du processus électoral, et les autres exigences associées à l'ouverture du logiciel.

7.4.1 AUTHENTICITÉ DU VOTANT

1. La plateforme de vote en réseau doit assurer l'identification des votants de façon unique (les votants doivent être distingués sans équivoque).
2. Un votant doit être en mesure de voter seulement dans la circonscription électorale dans laquelle il est inscrit.
3. La plateforme de vote en réseau doit être configurable de manière à exiger l'authentification une fois par contestation ou une fois par vote.
4. La plateforme de vote en réseau doit pouvoir authentifier les votants au moyen des méthodes d'authentification approuvées.
5. Les justificatifs d'identité du votant doivent être créés, distribués et protégés de manière à assurer leur secret.
6. Les justificatifs d'identité du votant doivent être assez solides pour ne pas pouvoir être obtenus ou devinés (par une attaque en force ou de l'information donnée au public).

7.4.2 SECRET DU VOTE

1. La plateforme de vote en réseau doit assurer que les votes déposés par les votants sont secrets.
2. Il doit être impossible de reconstruire un lien entre le votant et le contenu du vote. Cette règle s'applique non seulement lorsque le vote est déposé et archivé, mais aussi lorsque les votes sont dépouillés.
3. Sur confirmation au votant que le vote a bien été traité et archivé dans l'urne, le contenu du bulletin de vote ne doit pas être révélé dans un texte clair.
4. La plateforme de vote en réseau doit prévoir l'archivage et le chiffrement sécurisés des votes.
5. Les traces et les fichiers journaux des fonctions de vérification ne doivent révéler aucune information concernant le votant et le contenu du vote, et il doit être impossible d'utiliser ces fichiers journaux pour relier le votant à son vote.
6. La plateforme de vote en réseau doit assurer le secret des votes à tous les stades de l'élection, même si elle est terminée.
7. La plateforme de vote en réseau doit protéger la vie privée des votants. Tous les renseignements personnels (p. ex. Ceux qui figurent dans la liste électorale) des votants doivent être bien protégés.
8. L'information temporelle ou résiduelle gérée par les applications de vote (p. ex. Les témoins ou les fichiers temporels) doit être détruite après le dépôt du vote, ce qui supprime toute trace possible de l'information du votant ou des choix de vote.
9. Les mécanismes de sécurité utilisés pour protéger le secret et l'anonymat des votes (mots de passe ou clés cryptographiques, entre autres) doivent être utilisés et gérés de façon sécurisée, afin qu'il soit impossible de s'en servir pour mettre en péril le secret du vote.

7.4.3 CONTRÔLE DE L'ACCÈS AU SYSTÈME

1. L'accès aux composantes du vote en réseau doit être limité et archivé.
2. La plateforme de vote en réseau doit limiter l'accès à ses fonctionnalités et services publiés, d'après l'identité de l'utilisateur et le rôle accordé, aux fonctionnalités qui lui sont explicitement attribuées.
3. La plateforme de vote en réseau doit demander l'authentification de l'utilisateur avant l'exécution de toute action.
4. Les justificatifs d'identité de l'utilisateur doivent être secrets. Les comptes de l'utilisateur doivent reposer sur le principe du droit d'accès minimal.
5. La plateforme de vote en réseau doit protéger les données d'authentification de façon à ce que les entités non autorisées ne puissent mal utiliser, intercepter, modifier ou autrement connaître la totalité ou une partie de ces données.
6. Le processus et les procédures d'authentification doivent offrir des capacités de séparation des tâches.
7. Quiconque a accès à la plateforme de vote (agents électoraux, administrateurs d'élection, opérateurs ou vérificateurs) doit utiliser des mécanismes d'authentification solides, c.-à-d. des mécanismes d'authentification à double facteur.

7.4.4 INTÉGRITÉ DE L'ÉLECTION

1. Un seul vote valide doit être dépouillé par votant par élection.
2. La plateforme de vote en réseau doit empêcher d'insérer un vote directement dans l'urne.
3. La plateforme de vote en réseau doit empêcher de supprimer ou de modifier un vote dans l'urne.
4. Le système de vote dans un environnement à distance doit émettre un message pour indiquer au votant si le vote a été déposé avec succès – bien archivé dans l'urne – ou non.
5. La plateforme de vote en réseau doit assurer l'intégrité de l'urne en toutes circonstances.
6. La plateforme de vote en réseau doit assurer l'intégrité des votes archivés dans l'urne en toutes circonstances.
7. La plateforme de vote en réseau doit empêcher de modifier, de supprimer ou d'ajouter un vote contrefait pendant le transfert dans le réseau.
8. L'intégrité des données de configuration transmises à la plateforme de vote en réseau doit être protégée. L'authentification des données d'origine doit être assurée; elle inclut de l'information comme la liste électorale, la liste des candidats, ou toute autre information sur la configuration de l'élection.
9. La plateforme de vote en réseau doit transmettre un message de confirmation au votant lui indiquant que le vote a été archivé comme prévu. Cette confirmation doit être protégée contre la manipulation.
10. La plateforme de vote en réseau doit faire en sorte que le choix du votant est représenté avec exactitude dans le vote et que le vote scellé soit entré dans l'urne électronique.
11. Il devrait être impossible d'obtenir des résultats intermédiaires; il doit être impossible de connaître le nombre de votes déposés pour un candidat jusqu'à la fin du scrutin.

12. L'intégrité des données communiquées entre les modules de logiciel doit être maintenue.
13. L'intégrité des données communiquées à partir du stade préalable au vote (l'inscription des votants et les listes de candidats) doit être maintenue.
14. Il convient de s'assurer que le système de vote électronique présente un bulletin de vote authentique au votant. Dans le cas du vote électronique à distance, le votant doit être informé des moyens de vérifier qu'une connexion au serveur officiel a été établie et que le bulletin de vote authentique a été présenté.
15. Il convient de s'assurer qu'aucune donnée ne sera perdue en permanence advenant une panne ou une défaillance touchant le système de vote électronique.

7.4.5 DISPONIBILITÉ DU SERVICE

1. La plateforme de vote en réseau doit mettre en œuvre des mécanismes (comme la redondance) pour protéger la disponibilité des services pendant tout le processus de l'élection. Ces mécanismes doivent pouvoir résister, notamment, aux défaillances de système, aux pannes, ainsi qu'aux attaques entraînant un refus de service.
2. En cas de redémarrage du système, le système doit être remis rapidement au dernier statut compatible de la plateforme.
3. La plateforme de vote en réseau doit vérifier régulièrement si les composantes fonctionnent comme prévu.
4. L'authenticité, la disponibilité et l'intégrité des registres de votants et des listes de candidats doit être maintenue.

7.4.6 PROTECTION DU SERVICE

1. il doit y avoir une évaluation du risque de la plateforme de vote électronique, qui actualise sans cesse un modèle de gestion des menaces énumérant les menaces et les vulnérabilités recensées et les mesures d'atténuation correspondantes, et qui utilise systématiquement ces données au cours de cycle de développement du système pour atténuer les vulnérabilités recensées.
2. Lorsque des techniques cryptographiques sont utilisées, les clés cryptographiques privées ou secrètes doivent être fortement protégées.
3. Tous les modules de la plateforme de vote en réseau doivent être bien protégés contre le piratage, les logiciels malveillants, quels qu'ils soient, et toutes autres attaques.
4. La plateforme de vote en réseau doit maintenir des sources temporelles synchronisées qui soient fiables. L'exactitude de la source temporelle doit être suffisante pour préserver des repères de temps aux fins des vérifications rétrospectives et des données d'observation, et pour préserver les limites de temps aux fins de l'inscription, de la nomination, du vote ou du dépouillement.

7.4.7 VÉRIFICATION ET COMPTABILITÉ OUVERTES

1. La plateforme de vote en réseau doit fournir au votant une preuve de bout en bout que le vote a été reçu, enregistré et dépouillé comme le souhaitait le votant (sans enfreindre l'exigence de protection de la vie privée).
2. La plateforme de vote en réseau doit produire des traces ou fichiers journaux fiables qui soient assez détaillés pour pouvoir vérifier l'élection. Il faut assurer l'authenticité, la disponibilité, l'intégrité et la pertinence des données de vérification.
3. La vérification de bout en bout d'un système de vote électronique doit inclure l'enregistrement, la fourniture d'installations de surveillance et de vérification.
4. Le dépôt d'un vote dans les délais prévus doit être vérifiable.
5. Le système de vérification doit être ouvert et exhaustif, et faire rapport des menaces et des problèmes possibles.
6. Tous les modules de la plateforme de vote en réseau doivent être vérifiables.
7. Le système de vérification doit fournir la capacité de vérifier qu'une élection ou un référendum électronique s'est conformé aux dispositions légales applicables, dans le but de s'assurer que les résultats représentent avec exactitude les votes authentiques.
8. Le système de vérification doit offrir la capacité de contre-vérifier et de vérifier le fonctionnement correct du système électoral et l'exactitude du résultat, de repérer une fraude d'un votant et de prouver que tous les votes dépouillés sont authentiques et que tous les votes valides ont été dépouillés.
9. Avant la tenue d'une élection, la plateforme de vote en réseau doit permettre aux représentants électoraux, aux observateurs ou aux vérificateurs de vérifier que le système électoral est réel et fonctionne bien. Il doit être possible de s'assurer que seuls les logiciels approuvés et vérifiés sont exécutés.
10. Le système de vérification doit être protégé contre les attaques qui peuvent corrompre, modifier ou perdre des fichiers se trouvant dans le système de vérification.

8. MÉTHODOLOGIE D'ÉVALUATION DU RISQUE

Le modèle de vote en réseau présenté par cette étude de cas a été choisi sur la base d'une étude détaillée des technologies disponibles et des besoins, des buts et des contraintes spécifiques d'élections Ontario. Néanmoins, le vote en réseau présente un ensemble unique de risques qui doivent être évalués et gérés.

Pour évaluer le niveau de risque présenté par le modèle de vote en réseau recommandé par la présente étude de cas, certaines menaces potentielles ont été relevées. Dans le cas de chaque menace, les facteurs suivants ont alors été évalués :

Complexité : une cote des compétences techniques requises pour mener l'attaque. Règle générale, plus l'attaque est complexe, moins elle est susceptible de survenir.

Impact : une cote de l'effet de l'attaque si elle devait se produire.

Risque : le niveau de risque qui subsisterait après la mise en œuvre de mesures de prévention appropriées.

8.1 COMPLEXITÉ / PROBABILITÉ

Si un acteur malveillant mène une attaque technique, la probabilité que la menace pour la sécurité qui en résulte se concrétise est liée directement à la complexité de l'attaque potentielle et aux compétences et au niveau d'accès requis. En ce qui concerne ces types de menaces, la complexité de l'attaque potentielle est citée de un à cinq. Pour ce qui est des autres types de menace, dans le cadre desquelles il n'y aurait pas d'acteur responsable d'une attaque technique, on a recours à une évaluation de la probabilité pour compléter l'analyse. Les valeurs utilisées pour coter ces facteurs sont indiquées dans le tableau qui suit :

COMPLEXITÉ / PROBABILITÉ	
1- Très complexe / Très faible	Très complexe : Nécessite un niveau de compétences techniques très élevé combiné à un très grand effort. Très peu probable.
2- Complexe / Faible	Complexe : Nécessite un niveau de compétences techniques très élevé ou un très grand effort. Improbable.
3 – Standard / Moyenne	Standard : Nécessite un niveau de compétences techniques élevé ou un effort important. Il est difficile de prévoir si cela se produira ou non.
4 – Facile / Élevée	Facile : Nécessite seulement un niveau de compétences techniques de base avec un minimum d'efforts. Susceptible de survenir régulièrement.
5 – Très facile / Très élevée	Très facile : Tout utilisateur est en mesure de réaliser l'attaque. Très susceptible de survenir, très fréquent.

8.2 IMPACT

Pour chaque menace, l'impact potentiel est également coté. Les valeurs utilisées pour coter les facteurs de l'impact sont indiquées dans le tableau qui suit :

IMPACT	
1 – Très faible	Impact très faible : L'information n'est ni divulguée ni modifiée. La perception publique du SVR peut être touchée négativement, mais il n'y a pas d'impact sur l'élection.
2 - Faible	Faible impact : de l'information non cruciale est divulguée. Des bureaux de vote ou des votants peuvent être touchés.
3 - Moyen	Impact moyen : le contenu de certains votes pris au hasard pourrait être divulgué, ou le système de vote en réseau est temporairement indisponible. Un mode de scrutin complet pourrait être touché (c.-à-d. des bureaux de vote (ou la totalité d'entre eux)). Un grand groupe de votants peuvent être touchés.
4 - Élevé	Impact élevé : des bulletins de vote peuvent être modifiés, le contenu de certains votes peut être divulgué, ou le système de vote en réseau est indisponible à des moments cruciaux. Toute l'élection peut être touchée (tous les modes de scrutin). tous les votants peuvent être touchés, ce qui occasionne des difficultés mineures ou une indisponibilité pour une courte période (par exemple, un bref retard dans l'heure du début de l'élection).
5 – Très élevé	Impact très élevé : les résultats de l'élection sont sérieusement mis en péril, la confidentialité de l'urne est rompue, ou le système de vote est indisponible en permanence. Toute l'élection peut être touchée (tous les modes de scrutin). tous les votants peuvent être touchés, ce qui occasionne des difficultés majeures ou une indisponibilité pour une longue période (incapacité de lancer l'élection).

8.3 NIVEAU DE RISQUE RÉSIDUEL

Après avoir pris en compte la complexité ou la probabilité d'une menace potentielle et avoir combiné ce facteur avec l'impact probable de la menace, il existe un risque inhérent. Il y a quatre techniques de gestion du risque qui sont acceptées :

Évitement : éliminer le risque en évitant l'activité qui le produit.

Réduction : optimiser les approches de mise en œuvre pour atténuer le risque et réduire la probabilité, l'impact, ou les deux.

Partage : transférer le risque à d'autres parties par l'impartition, les partenariats, etc.

Rétention : accepter le risque et dresser un plan et un budget pour faire face aux conséquences.

En raison du caractère crucial du système de vote, la meilleure approche dans le présent cas est de diminuer chaque risque en mettant en œuvre des mesures de protection atténuantes. Pour chaque menace, une section sur l'atténuation décrit en conséquence les mesures de contrôle ou de protection qui peuvent effectivement faire diminuer le niveau de risque[17].

Comme il existe des mesures de protection ou des stratégies d'atténuation efficaces pour la plupart des menaces, cette évaluation cote le niveau de ***risque résiduel*** qui subsiste une fois que des mesures de protection adaptées à une attaque ou menace potentielle ont été mises en œuvre.

Les valeurs du risque possibles sont indiquées dans le tableau qui suit :

RISQUE	
1 – Très faible	Niveau de risque résiduel très faible, prise en compte d'un risque acceptable pour toute tolérance à un niveau de risque.
2 – Faible	Faible niveau de risque résiduel.
3 – Moyen	Niveau de risque résiduel moyen, considéré modéré.
4 – Élevé	Niveau de risque résiduel élevé, car **soit** la probabilité **soit** l'impact est élevé et il n'y a pas de mesures de protection efficaces pour contrer cette situation.
5 – Très élevé	Niveau de risque résiduel très élevé, car la probabilité et l'impact sont très élevés et il n'y a pas de mesures de protection efficaces pour le réduire. Les résultats de l'élection pourraient être mis en péril ou le système pourrait être indisponible en permanence.

9. ÉVALUATION DU RISQUE

Le présent chapitre donne les résultats d'une évaluation détaillée des risques rattachés aux quatre scénarios de vote en réseau de la liste retenue. Pour obtenir des détails sur la méthodologie employée pour évaluer le risque, veuillez vous reporter au chapitre précédent.

TYPES DE RISQUE

Le présent chapitre est structuré en trois grandes sous-sections, chacune portant sur un type de risque en particulier :

Évaluation du risque en matière de sécurité : analyse les risques surtout techniques qui pourraient toucher la sécurité du processus et de la plateforme de vote en réseau.

Évaluation du risque pour les opérations : analyse les risques essentiellement procéduraux pouvant survenir à divers niveaux des opérations.

Évaluation du risque pour le votant : analyse les risques propres au mode d'interaction des personnes avec le système et les processus connexes.

Chaque sous-section renferme un certain nombre de menaces, qui représentent des vulnérabilités potentielles devant être comprises et gérées. L'analyse de chaque menace inclut une définition de la complexité de l'attaque ou de la probabilité que la menace se concrétise; une évaluation du niveau d'impact engendré si la menace n'était pas gérée; les étapes détaillées de l'atténuation de la menace; et un niveau de risque résiduel évalue le niveau de risque qui subsiste une fois prises les démarches d'atténuation.

La figure qui suit donne un aperçu d'une analyse de menace type :

Description de la menace, complexité et impact, façons de gérer le risque, risque résiduel

Menace 1 : un pirate externe pourrait intercepter les communications entre l'ordinateur de vote et les serveurs de l'élection pour accéder au contenu du vote.

Complexité / Probabilité : Moyen

L'interception de voies de communications n'est pas une tâche négligeable : elle nécessite une connaissance appropriée et des outils particuliers.

IMPACT : ÉLEVÉ

Quiconque intercepte les voies de communications pourrait prendre connaissance des votes durant cette période.

Atténuation :

- Le système doit protéger les votes (p. ex. par le chiffrement) dans le terminal de votation du votant avant qu'ils soient transmis au serveur de l'élection (2.1.1.a, 2.1.4.b).
- Le système doit garantir que les votes sont chiffrés d'une façon que seul le conseil de gestion du vote en réseau peut déchiffrer (2.1.2.a, 2.1.4.c).
- Le système doit garantir que seul el conseil de gestion du vote en réseau peut déchiffrer les votes, après l'élection, idéalement dans un milieu isolé (p. ex. Sans être branché à un réseau de communication) (2.1.1.b).

- le système doit garantir que deux votes différents dont le contenu est identique présentent des formats de chiffrement différents (2.1.2.e).
- le système doit garantir que la clé nécessaire pour déchiffrer les votes n'est pas disponible pendant le processus de vote jusqu'à ce que le conseil de gestion du vote en réseau la retire/la reconstitue (2.1.2.b).
- le système doit garantir qu'au moins une majorité établie au préalable des membres du conseil de gestion du vote en réseau est nécessaire pour retirer la clé de déchiffrement de l'élection (2.1.2.c).
- le système doit garantir qu'un bulletin de vote déposé demeure secret devant les tiers, dont les administrateurs de système et les pirates éventuels qui franchissent les mesures de sécurité traditionnelles qui protègent la plateforme de vote (2.1.4.a).
- lorsque c'est possible, il convient d'avoir recours au chiffrement dans les voies de communications (1.2.5.e).

Risque : TRÈS FAIBLE

Comme le vote sera fortement chiffré dès la sélection, le niveau de risque résiduel sera très faible.

9.1 ÉVALUATION DU RISQUE EN MATIÈRE DE SÉCURITÉ

Organisation de la présente section

La présente section est structurée en fonction des cinq étapes de base du processus. Chaque sous-section traite des menaces possibles qui sont liées à chaque étape du processus, et expose une analyse du risque et des stratégies d'atténuation pour chaque menace.

- **Inscription et authentification**

  Cette section renferme les risques liés à la procédure d'authentification (sur la base de l'authentification de l'ID physique ou du mot de passe), et les mesures de prévention nécessaires pour les ramener à un niveau acceptable.

- **Vote**

  Cette section traite des risques et des mesures de contrôle qui s'appliquent à la période pendant laquelle les votants votent.

  Dans ce cas, il y a deux sections :

  - une pour le vote par ordinateur;
  - une pour le vote par téléphone.

- **Archivage des votes et gestion de l'urne**

  Cette section traite des risques et des mesures de prévention liées à la protection de l'urne électronique du début du scrutin à l'ouverture de l'urne pour procéder à la compilation.

- **Compilation**

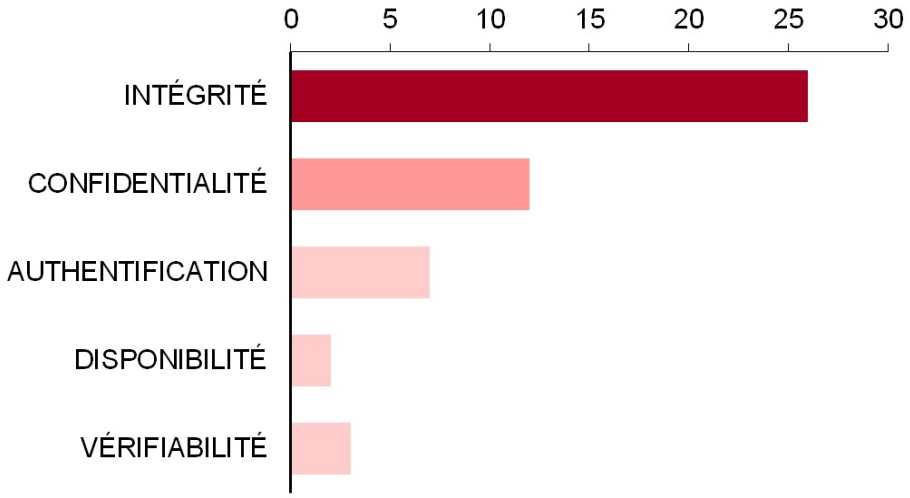
  La section sur la compilation intègre tous les risques et les mesures de contrôle liés à la révision des votes et au processus de dépouillement.

- **Vérification de l'élection**

  La dernière section porte sur les risques et les mesures de contrôle liés à la capacité de revoir le système électoral, et à son ouverture et sa transparence.

Catégories de risque

Figure 9: Catégories de risque



Une approche de vote en réseau qui englobe le vote par ordinateur et par téléphone est susceptible d'être vulnérable à plusieurs types de risques en matière de sécurité. Comme l'illustre le graphique à la droite expliqué dans la section suivante, le premier groupe de risques est formé des menaces contre l'exactitude des résultats, qui auraient une incidence directe sur l'intégrité de l'élection. Ces menaces comprennent la possibilité que les votes soient modifiés ou supprimés pendant qu'ils sont déposés, une fois qu'ils sont archivés dans le système, ou au moment de leur dépouillement.

Ensuite, diverses menaces portant sur la création d'un lien entre le votant et le suffrage exprimé peuvent affecter la confidentialité du vote. En outre, si les protocoles d'authentification ne sont pas suffisamment sécurisés, l'identité des votants pourrait être usurpée ou le nom de personnes n'ayant pas les qualités requises pour voter pourrait être ajouté à la liste des votants. Les risques d'un potentiel déni de service peuvent également compromettre la disponibilité du système pendant le vote, ainsi que les données requises pour assurer la vérifiabilité de l'élection.

Sommaire des résultats

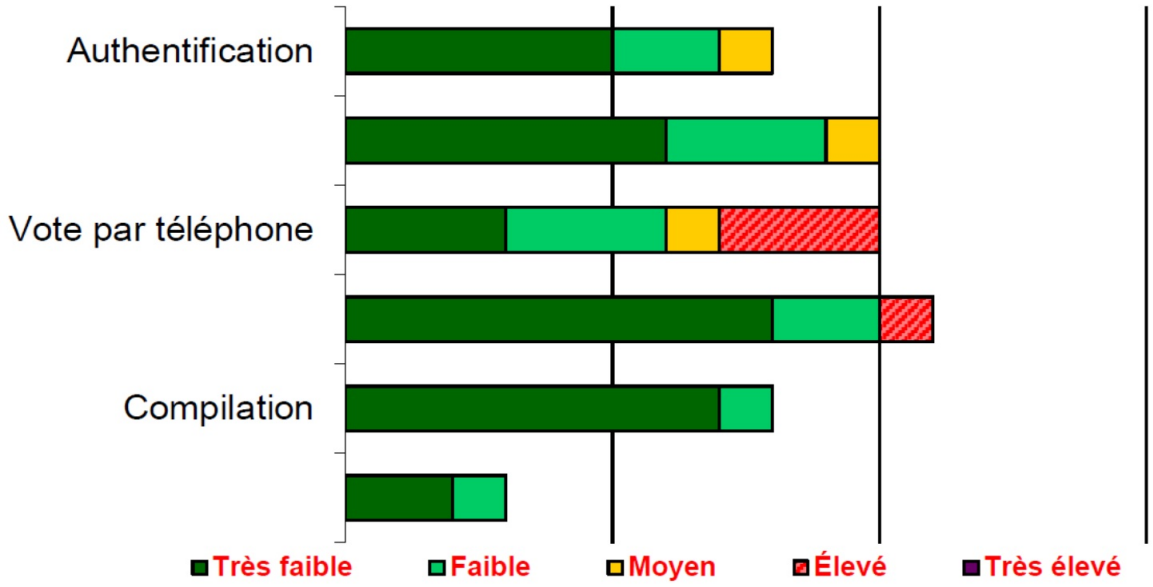
Le diagramme ci-contre synthétise l'évaluation des risques en matière de sécurité des quatre scénarios de vote en réseau. Il illustre le nombre de menaces potentielles à chaque étape du processus électoral et comporte deux lignes : une pour chaque mode de scrutin. Ce diagramme indique également le niveau de risque résiduel, sous réserve de la mise en œuvre des mesures d'atténuation appropriées.

Dans la majorité des cas, les menaces peuvent être atténuées de manière à limiter le risque résiduel à un niveau faible, voire très faible. Certains risques restent à un niveau moyen sur des points comme l'authentification par téléphone et le vote sous la contrainte.

La seule étape du processus présentant un risque résiduel élevé concerne le vote par téléphone, en raison des trois menaces majeures suivantes :

- interception du suffrage par un pirate entre l'appel téléphonique et le moment où le bulletin de vote est archivé sur les serveurs sécurisés de l'élection;
- interception des suffrages par un administrateur du système RVI pendant le transit, ce qui est contraire au principe de confidentialité et constitue une publication non autorisée;
- interception et modification des suffrages par un pirate.

Figure 10 : Niveaux de risque résiduel par étape du processus



Résultats par scénario

En outre, comme les quatre scénarios retenus de la liste qui sont analysés dans cette étude de cas présentent des cotes de risque différentes, le graphique qui suit illustre l'évaluation du risque pour chaque scénario analysé.

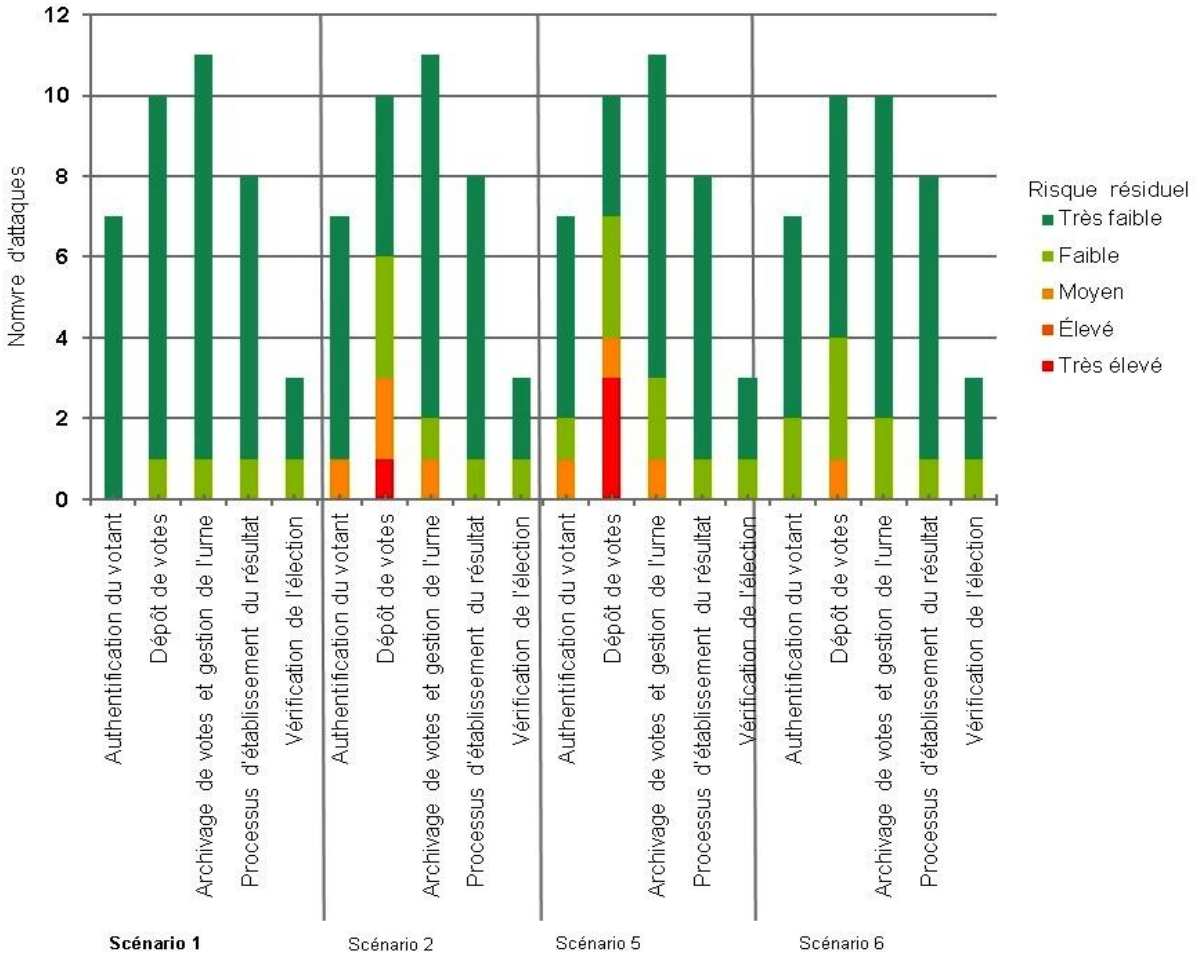
Scénario 1 : Vote sur site par ordinateur avec authentification basée sur une identification physique.

Scénario 2 : Vote sur site par téléphone avec authentification basée sur une identification physique.

Scénario 5 : Vote à distance par téléphone avec authentification basée sur un mot de passe.

Scénario 6 : Vote à distance par ordinateur avec authentification basée sur un mot de passe.

Figure 11: Évaluation des risques en matière de sécurité (par scénario)



9.1.1 RISQUES LIÉS À L'AUTHENTIFICATION DES VOTANTS

- Les menaces au niveau de l'authentification du votant sont essentiellement causées par des risques créés par la sécurité insuffisante du système :
- Les personnes autres que les votants admissibles peuvent entrer dans le système et voter, en contournant ou en contrant une procédure d'entrée en communication faible;
- Les justificatifs d'identité du votant pourraient être interceptés et un votant admissible pourrait faire l'objet d'une usurpation d'identité;
- Les règles sur la circonscription électorale dans laquelle le votant est admissible à voter ne sont pas bien appliquées;
- Des noms non autorisés sont ajoutés à la liste électorale.

9.1.1.1 USURPATION D'IDENTITÉ DU VOTANT (AUTHENTICITÉ DU VOTANT)

Un votant ou un pirate pourrait tenter de déposer un vote au nom d'une autre personne ou au nom de plusieurs personnes.

Menace 1 : Un pirate pourrait voler tous les justificatifs d'identité du votant dans les serveurs de l'élection, et déposer des votes valides au nom de votants autorisés.

Complexité : ÉLEVÉE

La capacité d'accéder aux serveurs de l'élection et de voler des justificatifs d'identité de vote nécessitera des compétences techniques avancées.

Impact : TRÈS ÉLEVÉ

Les votes non autorisés pourraient être traités à très grande échelle, et les résultats de l'élection pourraient être gravement mis en péril.

Atténuation :

- Les justificatifs d'identité du votant doivent être combinés aux données personnelles pour donner accès au système de vote afin de déposer un bulletin de vote (1.2.2.b).
- Le système doit avoir recours à des certificats numériques uniques pour authentifier les votants (2.1.9.g).
- Le fournisseur de service est chargé de déployer le logiciel requis et le système d'exploitation (y compris les serveurs de l'application, les bases de données, etc.), ainsi que de la configuration et du renforcement du système d'exploitation (2.3.6.d).

Risque : TRÈS FAIBLE

Comme les justificatifs d'identité qui se trouvent dans les serveurs de l'élection, qui archivent les justificatifs d'identité, seront chiffrés et fortement protégés, le niveau de risque résiduel sera très faible.

Menace 2 : Un pirate pourrait tenter d'obtenir des justificatifs d'identité du votant valides (en les devinant, ou par des attaques en force ou en interceptant un appel téléphonique) et de déposer un vote valide au nom de votants autorisés.

Complexité : FACILE

Une fois que les justificatifs d'identité sont générés et archivés de façon sécurisée dans le système de vote, des attaques pourraient être faites pour tenter de simuler l'utilisation, par un votant, d'interfaces externes (p. ex. En devinant un justificatif d'identité ou en faisant une attaque en force) **ou** en interceptant de faibles communications internes (p. ex. Le segment VRI). Des compétences techniques de base seraient nécessaires pour mener une attaque en force. Un administrateur VRI pourrait avoir accès à l'information en surveillant les appels lors d'un vote par téléphone.

Impact : ÉLEVÉ

Les votes non autorisés pourraient être traités comme étant valides, ce qui affecterait les résultats de l'élection.

Atténuation :

- Les justificatifs d'identité du votant doivent être combinés aux données personnelles pour donner accès au système de vote afin de déposer un bulletin de vote (1.2.2.b).
- Le système doit avoir recours à des certificats numériques uniques pour authentifier les votants (2.1.9.g).
- Les procédures appropriées sont en place pour garantir que les opérateurs techniques VRI n'ont pas accès au système pendant le processus de vote, sauf s'il survient quelque chose de crucial (p. ex. Si un redémarrage du système est nécessaire).
- Des mesures appropriées sont en place pour éviter les attaques externes et le reniflage de réseau.
- Il est à noter qu'un pirate qui pourrait intercepter un vote par téléphone pourrait également intercepter les justificatifs d'identité des votants qui utilisent le téléphone, et usurper leur identité. toutefois, le votant s'en rendrait compte ultérieurement parce qu'il serait incapable de voter (sauf si des votes multiples par votant sont autorisés).

Risque : FAIBLE pour le vote par ordinateur; MOYEN pour le vote par téléphone.

Si des mesures de contrôle suffisantes sont en place, le niveau de risque résiduel sera faible dans le cas du vote par ordinateur, mais MOYEN dans le cas du vote par téléphone.

Menace 3 : Un pirate pourrait voler les justificatifs d'identité du votant, et déposer un vote valide au nom du votant autorisé.

Complexité : COMPLEXE

Si les justificatifs d'identité ne sont pas générés et archivés dans le système de vote de manière sécurisée, ils pourraient être vulnérables aux attaques de travailleurs en place malveillants ou de pirates externes qui ont accès aux serveurs.

Il faudrait déployer un effort majeur pour voler les justificatifs d'identité du votant dans le système de vote, même dans le cas des administrateurs de système, s'ils sont protégés individuellement.

Impact : ÉLEVÉ

Les votes non autorisés pourraient être traités comme valides, ce qui affecterait les résultats de l'élection.

Atténuation :

- Le système doit pouvoir exporter des données pour fournir au processus de carte d'avis d'enregistrement (CAE) des données suffisantes pour charger et distribuer des ID d'électeur par courrier (1.1.2.c).
- Les justificatifs d'identité du votant doivent être combinés aux données personnelles pour donner accès au système de vote afin de déposer un bulletin de vote (1.2.2.b).
- Le système doit avoir recours à des certificats numériques uniques pour authentifier les votants (2.1.9.g).
- Les justificatifs d'identité du votant doivent être protégés si/quand ils sont archivés dans le système de vote.

Risque : FAIBLE

Comme le votant sera fortement authentifié, le risque d'usurpation d'identité sera faible, compte tenu du fait que les justificatifs d'identité du votant sont bien protégés.

9.1.1.2 LES VOTANTS NON AUTORISÉS QUI VOTENT (AUTHENTICITÉ DU VOTANT)

Les votants non admissibles pourraient exprimer un suffrage lors d'une élection en particulier.

Menace 1 : Une personne qui ne figure pas sur la liste officielle des votants pourrait exprimer un suffrage.

Complexité : FACILE

Si le système n'est pas assez sécurisé, une personne qui ne se trouve pas sur la liste des votants pourrait exprimer un suffrage.

Impact : ÉLEVÉ

Des votes non autorisés pourraient être traités, ce qui affecterait les résultats de l'élection.

Atténuation :

- Le système doit exiger que les votants se servent de justificatifs d'identité en particulier pour accéder au système de vote (1.2.2.a).
- Le système doit garantir que seuls les votants admissibles peuvent entrer dans la plateforme de vote (2.1.9.a).
- Avant d'accepter un vote déposé, le système doit vérifier l'identité du votant qui dépose le vote (2.1.9.b).
- Le système doit permettre de vérifier à tout moment pendant l'élection que les votes déposés dans l'urne sont bien ceux de votants admissibles (2.1.9.d).
- Le système doit empêcher l'ajout de bulletins de vote contrefaits dans l'urne par des utilisateurs externes et des administrateurs du système (2.1.9.f).
- Le système doit avoir recours à des certificats numériques uniques pour authentifier les votants (2.1.9.g).
- Le système doit utiliser des certificats numériques uniques du votant pour signer numériquement les votes déposés (2.1.9.h). Il est à noter que dans le cas du vote par téléphone, la signature est faite dans les serveurs plutôt que dans l'ordinateur du votant comme pour le vote par internet.

Risque : TRÈS FAIBLE

Comme des mesures de protection efficaces permettront de valider l'admissibilité des votants, le niveau de risque résiduel sera très faible.

Menace 2 : Un votant pourrait être en mesure de déposer un vote dans une circonscription électorale dans laquelle il n'est pas inscrit.

Complexité : FACILE

Toute personne pourrait tenter de déposer un vote, même pour une course qui a lieu à l'extérieur de la circonscription électorale dans laquelle elle est inscrite.

Impact : ÉLEVÉ

Des votes non autorisés pourraient être traités, ce qui affecterait les résultats de l'élection.

Atténuation :

- Le système doit exiger que les votants se servent de justificatifs d'identité en particulier pour accéder au système de vote (1.2.2.a).
- Le système doit garantir que seuls les votants admissibles peuvent entrer dans la plateforme de vote (2.1.9.a).
- Avant d'accepter un vote déposé, le système doit vérifier l'identité du votant qui dépose le vote (2.1.9.b).
- Le système doit permettre de vérifier à tout moment pendant l'élection que les votes déposés dans l'urne sont bien ceux de votants admissibles (2.1.9.d).
- Le système doit empêcher l'ajout de bulletins de vote contrefaits dans l'urne par des utilisateurs externes et des administrateurs du système (2.1.9.f).
- Le système doit avoir recours à des certificats numériques uniques pour authentifier les votants (2.1.9.g).
- Le système doit utiliser des certificats numériques uniques du votant pour signer numériquement les votes déposés (2.1.9.h).

Risque : TRÈS FAIBLE

Comme des mesures de protection efficaces permettront de vérifier l'admissibilité du votant à chaque élection, le niveau de risque résiduel sera très bas.

Menace 3 : Un pirate pourrait tenter de modifier la liste des votants gérée par l'application de vote pour se faire inclure comme votant admissible.

Complexité : MOYENNE

Le système de vote doit gérer sa propre liste des électeurs, qui sera importée des systèmes d'élections Ontario. Le pirate devrait posséder des compétences techniques considérables pour modifier la liste électorale.

Impact : TRÈS ÉLEVÉ

Des votes non autorisés pourraient être traités, ce qui affecterait les résultats de l'élection.

Atténuation :

- Le système doit vérifier que les données sur l'élection sont certifiées par le conseil de gestion du vote en réseau avant de lancer les processus de vote et de dépouillement (1.1.4.a).
- Tout vérificateur indépendant doit pouvoir certifier l'intégrité et l'authenticité des composantes du système installées dans la plateforme de vote (1.1.4.e).
- Le fournisseur de service doit être chargé de déployer le logiciel requis en plus du système d'exploitation (y compris les serveurs d'application, les bases de données, etc.), ainsi que de la configuration et du renforcement du système d'exploitation (2.3.6.d).

Risque : TRÈS FAIBLE

Comme toutes les composantes du système de vote – telle la liste électorale – seront protégées et signées numériquement, le niveau de risque résiduel sera très faible.

Menace 4 : Un pirate pourrait tenter – à titre de votant non admissible – de déposer un vote en contournant le processus d'authentification.

Complexité / Probabilité : MOYENNE

Il serait complexe de contourner le processus d'authentification.

Impact : ÉLEVÉ

Des votes non autorisés pourraient être traités comme valides, ce qui affecterait les résultats de l'élection.

Atténuation :

- Le système doit exiger que les votants se servent de justificatifs d'identité en particulier pour accéder au système de vote (1.2.2.a).
- Le système doit garantir que seuls les votants admissibles peuvent entrer dans la plateforme de vote (2.1.9.a).
- Avant d'accepter un vote déposé, le système doit vérifier l'identité du votant qui dépose le vote (2.1.9.b).
- Le système doit permettre de vérifier à tout moment pendant l'élection que les votes déposés dans l'urne sont bien ceux de votants admissibles (2.1.9.d).
- Le système doit empêcher l'ajout de bulletins de vote contrefaits dans l'urne par des utilisateurs externes et des administrateurs du système (2.1.9.f).
- Le système doit avoir recours à des certificats numériques uniques pour authentifier les votants (2.1.9.g).
- Le système doit utiliser des certificats numériques uniques du votant pour signer numériquement les votes déposés (2.1.9.h).

Risque : TRÈS FAIBLE

Comme des mesures de contrôle seront en place pour authentifier fortement les utilisateurs, le niveau de risque résiduel sera très faible.

9.1.2 LE VOTE PAR ORDINATEUR

Le dépôt de votes à l'aide d'un ordinateur, sur site ou à distance, donne lieu à plusieurs catégories de risque :

- La confidentialité pourrait être mise en péril;
- Il pourrait y avoir vote sous la contrainte ou achat de votes;
- Des votes pourraient être modifiés après leur dépôt;
- Des votes pourraient être supprimés après leur dépôt;
- Le votant pourrait se sentir incertain que son vote a été déposé.

9.1.2.1 MISE EN PÉRIL DE LA CONFIDENTIALITÉ (VIE PRIVÉE ET CONFIDENTIALITÉ DU VOTANT)

Un pirate pourrait violer la vie privée du votant, en reliant le votant et son choix de vote par les moyens suivants :

- en interceptant des communications entre l'ordinateur de vote et les serveurs;
- en accédant à l'infrastructure de vote en réseau directement de l'intérieur; et (ou)
- en installant un logiciel malveillant dans les ordinateurs de vote.

Menace 1 : Un pirate externe pourrait intercepter les communications entre l'ordinateur de vote et les serveurs de l'élection pour accéder au contenu du vote.

Complexité / Probabilité : MOYENNE

L'interception de voies de communications n'est pas une tâche négligeable : elle nécessite une connaissance appropriée et des outils particuliers.

Impact : ÉLEVÉ

Quiconque intercepte les voies de communications pourrait prendre connaissance des votes durant cette période.

Atténuation :

- Le système doit chiffrer les votes dans le terminal de votation du votant avant qu'ils soient transmis au serveur de l'élection (2.1.19.b).
- Le système doit garantir que les votes sont chiffrés d'une façon que seul le conseil de gestion du vote en réseau peut déchiffrer (2.1.18.a).
- Le système doit garantir que seul le conseil de gestion du vote en réseau peut déchiffrer les votes, après l'élection, idéalement dans un milieu isolé (p.ex., sans être branché à un réseau de communication) (1.3.2.a, 2.1.19a).
- Le système doit garantir que deux votes différents dont le contenu est identique présentent des formats de chiffrement différents (2.1.18.e).
- Le système doit garantir que la clé nécessaire pour déchiffrer les votes n'est pas disponible pendant le processus de vote jusqu'à ce que le conseil de gestion du vote en réseau la retire/la reconstitue (2.1.18.b).
- Le système doit garantir qu'au moins une majorité établie au préalable des membres du conseil de gestion du vote en réseau est nécessaire pour retirer la clé de déchiffrement de l'élection (2.1.18.c).

- Le système doit garantir qu'un bulletin de vote déposé demeure secret devant les tiers, dont les administrateurs de système et les pirates éventuels qui franchissent les mesures de sécurité traditionnelles qui protègent la plateforme de vote (2.1.18.a).
- Lorsque c'est possible, il convient d'avoir recours au chiffrement dans les voies de communications (1.2.5.e).

Risque : TRÈS FAIBLE

Comme le vote sera fortement chiffré dès la sélection, le niveau de risque résiduel sera très faible.

Menace 2 : Un administrateur de système d'une composante intermédiaire de l'infrastructure (p. ex. Les serveurs de l'élection) aurait accès aux votes au moyen des options de vote choisies par les votants.

Complexité : FACILE

Il serait facile pour un administrateur de système d'un serveur intermédiaire d'accéder aux données en transit.

Impact : ÉLEVÉ

Quiconque a accès aux composantes intermédiaires de l'infrastructure prendrait alors connaissance des votes.

Atténuation :

- Le système doit protéger les votes (p. ex. par le chiffrement) dans le terminal de votation du votant avant qu'ils soient transmis au serveur de l'élection (2.1.19.b).
- Le système doit garantir que seul le conseil de gestion du vote en réseau peut déchiffrer les votes, après l'élection, idéalement dans un milieu isolé (p.ex., sans être branché à un réseau de communication) (2.1.19.a).
- Le système doit garantir que les votes sont chiffrés d'une façon que seul le conseil de gestion du vote en réseau peut déchiffrer (2.1.18.a).
- Le système doit garantir que la clé nécessaire pour déchiffrer les votes n'est pas disponible pendant le processus de vote jusqu'à ce que le conseil de gestion du vote en réseau la retire/la reconstitue (2.1.18.b).
- Le système doit garantir qu'au moins une majorité établie au préalable des membres du conseil de gestion du vote en réseau est nécessaire pour retirer la clé de déchiffrement de l'élection (2.1.18.c).
- Le système doit garantir que deux votes différents dont le contenu est identique présentent des formats de chiffrement différents (2.1.18.e).

Risque : TRÈS FAIBLE

Comme le vote sera chiffré de la sélection du vote au déchiffrement, le niveau de risque résiduel sera très faible.

Menace 3 : Un logiciel malveillant exploité dans des ordinateurs utilisés pour accéder au système de vote en réseau pourrait servir à tenter d'accéder aux options de vote retenues par un votant.

Complexité : COMPLEXE

Des compétences techniques avancées seraient nécessaires pour installer un logiciel malveillant dans les ordinateurs des votants conçus expressément pour recenser les options de vote. Ce piratage est encore moins réalisable dans les terminaux de votation se trouvant dans des bureaux de vote.

Impact : MOYEN

Quiconque met en péril l'ordinateur pourrait prendre connaissance des votes déposés au moyen de ce terminal.

Atténuation :

- *Vote sur site par ordinateur :* le fournisseur de service doit décrire ses besoins en matériel, périphériques d'accessibilité, logiciel COTS, réseautage et dispositifs de sécurité pour assurer la disponibilité et la performance nécessaires. fournir des estimations pour les éléments de sauvegarde (2.3.3.b).
- *Vote sur site par ordinateur :* le fournisseur de service est chargé de déployer le logiciel requis en plus du système d'exploitation, et de la configuration et du renforcement du système d'exploitation et de la configuration des périphériques d'accessibilité. (2.3.3.d).
- *Vote à distance par ordinateur :* l'évaluation du risque qui a été effectuée a posé comme hypothèses que les ordinateurs personnels seront exempts de logiciels malveillants et dotés des logiciels anti espion, des logiciels anti maliciel et des outils antivirus adéquats.

Risque : FAIBLE

Bien que la protection des terminaux de votation contre les maliciels ait été améliorée, il subsiste certains risques que les maliciels ne soient pas détectés par les outils de sécurité (comme les logiciels antivirus).

9.1.2.2 VOTE SOUS LA CONTRAINTE ET ACHAT DE VOTES (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Une personne ou une organisation pourrait contraindre un votant à voter pour un candidat en particulier ou le soudoyer pour obtenir ce résultat par les moyens suivants :

- Le vote est supervisé par l'auteur de la contrainte.
- Le votant est en mesure, et peut donc être contraint, de montrer une preuve de son choix sur le bulletin de vote.

Menace 1 : Le votant pourrait exprimer un suffrage sous la surveillance d'une personne qui achète des votes ou exerce de la contrainte.

Complexité : FAIBLE

Il est possible mais non fréquent dans les démocraties bien établies d'acheter le vote d'une personne ou de la contraindre à voter avec une intention précise.

Impact : ÉLEVÉ

Une personne qui est en mesure de corrompre ou de contraindre un votant pourrait modifier l'exactitude des résultats.

Atténuation :

Le système doit produire des accusés de réception de vote qui ne permettent pas aux votants de prouver à un tiers pour qui ils ont voté (2.1.13.a).

Le système doit empêcher quiconque, même les gestionnaires et les vérificateurs protégés, d'établir une corrélation entre les votes et les votants (2.1.13.b).

Risque : MOYEN

Il est possible d'acheter un vote ou de contraindre un votant lorsqu'il vote à distance et qu'un membre du personnel de scrutin n'exerce pas de supervision. Cela s'applique à tout système de vote à distance ou non supervisé (comme le bulletin de vote postal).

Toutefois, les systèmes de vote en réseau permettent de mettre en œuvre des mesures particulières pour atténuer ce risque : permettre aux votants de voter plusieurs fois, et dépouiller seulement les derniers suffrages exprimés.

Menace 2 : Un votant peut montrer ses options de vote à une personne qui achète des votes ou fait voter sous la contrainte.

Complexité / Probabilité : FAIBLE

Le fait de corrompre ou de contraindre un votant pour l'amener à voter avec une intention précise est possible, mais n'est pas courant dans des démocraties bien établies.

Impact : ÉLEVÉ

Quiconque achète des votes ou fait voter sous la contrainte pourrait modifier l'exactitude des résultats.

Atténuation :

- Le système doit produire des accusés de réception de vote qui ne permettent pas aux votants de prouver à un tiers pour qui ils ont voté (2.1.13.a).
- L'accusé de réception du vote doit protéger le secret du vote (c.-à-d. que l'on ne devrait jamais pouvoir déduire les options de vote retenues) (2.1.14.b).
- Le système doit empêcher quiconque, même les gestionnaires et les vérificateurs protégés, d'établir une corrélation entre les votes et les votants (2.1.14.b).

Risque : TRÈS FAIBLE

Comme l'accusé de réception du vote ne renferme pas de renseignements concernant les options de vote retenues, le votant ne serait pas en mesure de montrer son choix.

9.1.2.3 MODIFICATION DU VOTE (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Le contenu du vote pourrait être changé pour modifier les résultats de l'élection en ayant recours aux moyens suivants :

- par l'installation d'un logiciel malveillant dans les ordinateurs de vote;
- par l'interception du trafic entre l'ordinateur de vote et le serveur de l'élection.

Menace 1 : Un logiciel malveillant exploité dans des ordinateurs utilisés pour accéder au système de vote en réseau pourrait modifier l'option de vote retenue par un votant.

Complexité / Probabilité : COMPLEXE

Des compétences techniques poussées et des connaissances approfondies du système de vote en réseau seraient nécessaires pour installer sur les ordinateurs des votants un logiciel malveillant qui est conçu expressément pour modifier leurs choix.

Impact : ÉLEVÉ

Des bulletins de vote pourraient être modifiés.

Atténuation :

- *vote sur site par ordinateur :* le fournisseur de service doit décrire ses besoins en matériel, périphériques d'accessibilité, logiciel COTS, réseautage et dispositifs de sécurité pour assurer la disponibilité et la performance nécessaires. fournir des estimations pour les éléments de sauvegarde (2.3.3.b).
- *vote sur site par ordinateur :* le fournisseur de service est chargé de déployer le logiciel requis en plus du système d'exploitation, et de la configuration et du renforcement du système d'exploitation et de la configuration des périphériques d'accessibilité. (2.3.3.d).
- *vote à distance par ordinateur :* l'évaluation du risque qui a été effectuée a posé comme hypothèses que les ordinateurs personnels seront exempts de logiciels malveillants et dotés des logiciels anti espion, des logiciels anti maliciel et des outils antivirus adéquats.

Risque : FAIBLE

Bien que la protection des terminaux de votation contre les maliciels ait été améliorée, il subsisterait certains risques que les outils de sécurité ne puissent détecter un programme. Toutefois, les compétences et l'effort exigés restreignent la faisabilité d'un piratage.

Menace 2 : Un piratage externe pourrait intercepter les communications entre l'ordinateur de vote et le serveur de l'élection, et modifier l'option de vote retenue par le votant.

Complexité / Probabilité : MOYENNE

L'interception de voies de communication n'est pas une tâche négligeable : elle nécessite une connaissance appropriée et des outils particuliers.

Impact : ÉLEVÉ

Des bulletins de vote pourraient être modifiés.

Atténuation :

- Le système doit protéger l'intégrité de chaque vote déposé pendant tout le processus électoral (2.1.15.a).
- Une cryptographie solide, qui a notamment recours à des signatures numériques, devrait protéger l'intégrité du vote (2.1.15.e).
- Dans le cas du vote par ordinateur, le système doit protéger la confidentialité et l'intégrité du vote déposé, de même que l'identité du votant, par des moyens cryptographiques, de manière à ce que le vote ne puisse être altéré pendant son transport ou son archivage (1.2.5.b).
- Dans le cas du vote par ordinateur, le système doit également permettre aux votants de protéger leurs votes dans leur ordinateur de vote avant de le déposer, plutôt que seulement lorsque les serveurs de l'élection reçoivent les votes (1.2.5.c).
- Les votes déposés doivent être protégés contre les attaques externes et internes (p. ex. par les administrateurs de système) en ayant recours à des mesures cryptographiques

adéquates pouvant être démontrées devant un expert en matière de sécurité ou un vérificateur (1.2.5.d).

Risque : TRÈS FAIBLE

Comme le vote fera l'objet d'une signature numérique dès le choix des candidats, le niveau de risque résiduel sera très faible.

9.1.2.4 SUPPRESSION DU VOTE (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Un pirate pourrait tenter de supprimer des votes valides en interceptant les bulletins de vote et en les empêchant de se rendre aux serveurs de l'élection.

Menace 1 : Un pirate externe pourrait intercepter le vote une fois qu'il a quitté l'ordinateur de vote et l'empêcher de se rendre avec succès au serveur de l'élection, tout en laissant croire au votant que le bulletin de vote a été déposé avec succès.

Complexité / Probabilité : MOYENNE

L'interception de voies de communication n'est pas une tâche négligeable : elle nécessite une connaissance appropriée et des outils particuliers.

Impact : ÉLEVÉ

Des bulletins de vote pourraient être supprimés.

Atténuation :

- Le système doit fournir aux votants un accusé de réception une fois qu'ils ont déposé leur vote. Cet accusé de réception leur permettra de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de dépouillement (1.2.6.a).
- Le système doit permettre aux votants de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de compilation au moyen d'un accusé de réception (2.1.14.a).
- Les voies de communications doivent être protégées par le chiffrement (1.2.5.e).

Risque : TRÈS FAIBLE

Comme le vote sera confirmé par un accusé de réception vérifiable, le risque résiduel de suppression d'un vote en transit sera très faible.

9.1.2.5 INCERTITUDE DU VOTANT QUANT AU BULLETIN DE VOTE DÉPOSÉ (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Si un votant ne dispose pas d'une façon de vérifier la réception et le dépouillement corrects de son vote, le votant pourrait commencer à éprouver de l'incertitude quant au processus électoral.

Menace 1 : Le votant pourrait douter que son vote a été archivé dans l'urne.

Probabilité : ÉLEVÉ

Il est très possible qu'un votant soit incertain que son vote électronique a été archivé correctement dans l'urne.

Impact : ÉLEVÉ

L'élection peut perdre de la crédibilité.

Atténuation :

- L'écran du bulletin de vote en ligne ou le menu RVI doit être assez utilisable pour que les votants puissent distinguer clairement leurs choix et être mis en garde contre des choix faits par mégarde ou d'autres erreurs (1.2.4.g, 1.2.4.h, 2.1.2.e).
- Le système doit fournir aux votants un accusé de réception une fois qu'ils ont déposé leur vote. Cet accusé de réception leur permettra de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de dépouillement (1.2.6.a).
- Le système doit permettre aux votants de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de compilation au moyen d'un accusé de réception. (2.1.14.a).
- Le processus de vérification doit permettre de détecter les accusés de réception manipulés ou contrefaits pour empêcher les déclarations frauduleuses des votants (2.1.14.c).

Risque : TRÈS FAIBLE

Comme le votant aura un accusé de réception et pourra s'assurer que son bulletin de vote a été dénombré, le niveau de risque résiduel sera très faible.

Menace 2 : Le votant pourrait avoir l'impression que son vote n'a pas été déposé adéquatement.

Probabilité : ÉLEVÉE

Il est très possible que de nombreux votants estiment que leur vote n'a pas été déposé adéquatement.

Impact : ÉLEVÉ

Les élections pourraient ne pas avoir suffisamment de crédibilité aux yeux des citoyens et d'autres parties prenantes.

Atténuation :

- L'écran du bulletin de vote en ligne ou le menu RVI doit être assez utilisable pour que les votants puissent distinguer clairement leurs choix et être mis en garde contre des choix faits par mégarde ou d'autres erreurs. (1.2.4.g, 1.2.4.h, 2.1.2.e).
- Le système doit fournir aux votants un accusé de réception une fois qu'ils ont déposé leur vote. Cet accusé de réception leur permettra de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de dépouillement (1.2.6.a).
- Le système doit permettre aux votants de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de compilation au moyen d'un accusé de réception. (2.1.14.a).
- Le processus de vérification doit permettre de détecter les accusés de réception manipulés ou contrefaits pour empêcher les déclarations frauduleuses des votants (2.1.14.c).

Risque : FAIBLE

Comme le votant disposera d'un accusé de réception et pourra s'assurer que son bulletin de vote a été dépouillé, le niveau de risque résiduel sera faible.

9.1.3 LE VOTE PAR TÉLÉPHONE

Le vote par téléphone comprend les mêmes catégories de risque que le vote par ordinateur, mais les menaces et les facteurs d'atténuation diffèrent :

- la confidentialité pourrait être mise en péril;
- il pourrait y avoir vote sous la contrainte ou achat de votes;
- des votes pourraient être modifiés après leur dépôt;
- des votes pourraient être supprimés après leur dépôt;
- le votant pourrait se sentir incertain que son vote a été déposé.

9.1.3.1 MISE EN PÉRIL DE LA CONFIDENTIALITÉ (VIE PRIVÉE ET CONFIDENTIALITÉ DU VOTANT)

Un pirate pourrait violer la vie privée du votant, en reliant le votant et son choix de vote par les moyens suivants :

- en interceptant des communications entre le téléphone de vote et les serveurs;
- en accédant à la RVI ou à l'infrastructure de vote en réseau directement de l'intérieur;
- en installant un logiciel malveillant dans les téléphones utilisés pour voter.

Menace 1 : un pirate externe pourrait intercepter les communications entre le téléphone et le RVI, ou entre le RVI et les serveurs de l'élection sécurisés.

Complexité / Probabilité : MOYENNE

L'interception de voies de communications téléphoniques n'est pas une tâche négligeable : elle nécessite une connaissance appropriée, des outils particuliers et un point d'accès précis pour surveiller le réseau téléphonique. Toutefois, les communications entre le RVI et les serveurs de l'élection sécurisés sont un peu plus faciles à intercepter.

Impact : ÉLEVÉ

Quiconque est parvenu à intercepter les voies de communications serait alors en mesure de prendre connaissance des votes déposés.

Atténuation :

Lorsque c'est possible, il convient d'avoir recours au chiffrement dans les voies de communications (1.2.5.e).

Risque : ÉLEVÉ

Comme les voies de communications téléphoniques ne permettent pas le chiffrement, un vote par téléphone n'est pas chiffré tant qu'il n'est pas arrivé à un serveur intermédiaire. dans le cas des téléphones analogiques, les voies de communications (RTCP) ne permettent pas le chiffrement de la voie; dans le cas des téléphones cellulaires, l'information est chiffrée lorsqu'elle se dirige vers la station de relais, mais est alors transmise sans être chiffrée à la plateforme VRI; dans le cas d'un téléphone IP, l'information est toujours chiffrée, mais un administrateur de système pourrait voir clairement toute l'information transmise dans les passerelles VoIP, y compris les messages sonores et les options retenues. En conséquence, le niveau de risque résiduel sera élevé.

Menace 2 : L'administrateur de système d'une composante d'infrastructure intermédiaire (plateforme VRI …) aurait accès aux votes en transit, et pourrait donc prendre connaissance des options de vote des votants.

Complexité / Probabilité : FACILE

L'administrateur de système d'un serveur intermédiaire peut facilement accéder aux données en transit.

Impact : ÉLEVÉ

Un acteur qui intercepte les voies de communications prendrait connaissance des votes déposés pendant cette période.

Atténuation :

- le fournisseur de service doit être chargé de déployer le logiciel requis en plus du système d'exploitation (y compris les serveurs d'application, les bases de données, etc.), ainsi que de la configuration et du renforcement du système d'exploitation (2.3.6.d).
- lorsque c'est possible, il convient d'avoir recours au chiffrement dans les voies de communications (1.2.5.e).
- déployer les procédures appropriées pour détecter un administrateur de VRI ou d'autres utilisateurs non autorisés qui ont accès la plateforme et au réseau pendant la période de vote.

Risque : élevé

Quoique la plateforme VRI fasse l'objet d'un processus de renforcement de la sécurité, les mesures de contrôle efficaces ne seront pas suffisantes pour garantir qu'un administrateur de plateforme VRI n'aura pas accès aux options de vote en transit, car elles ne sont pas chiffrées. Par conséquent, le niveau de risque résiduel demeurera élevé.

Menace 3 : Un logiciel malveillant dans les terminaux de votation permet d'avoir accès aux options de vote retenues par les votants.

Complexité / Probabilité : TRÈS COMPLEXE

Il faudrait des compétences techniques très poussées, combinées à un effort très considérable, afin d'installer un logiciel malveillant sur des appareils téléphoniques pour accéder aux options de vote et les archiver. À l'heure actuelle, seuls certains téléphones mobiles sont visés par un nombre limité de maliciels, et ils touchent seulement les modes de scrutin basés sur des données, et non sur la voix.

Impact : MOYEN

Quiconque met en péril le terminal téléphonique pourrait prendre connaissance des votes déposés par ce terminal.

Atténuation :

- *Vote sur site par téléphone* : le fournisseur de service doit décrire ses besoins en matériel, périphériques d'accessibilité, logiciel COTS, réseautage et dispositifs de sécurité pour assurer la disponibilité et la performance nécessaires. fournir des estimations pour les éléments de sauvegarde (2.3.3.b).

- *Vote sur site par téléphone* : le fournisseur de service est chargé de déployer le logiciel requis en plus du système d'exploitation, et de la configuration et du renforcement du système d'exploitation, et de la configuration des périphériques d'accessibilité. (2.3.3.d).
- *Vote à distance par téléphone* : l'évaluation du risque qui a été effectuée pose comme hypothèses que les téléphones personnels sont des téléphones courants non branchés à des sources de maliciel.

Risque : TRÈS FAIBLE

Le niveau de risque résiduel sera très faible en raison de la complexité du piratage téléphonique par maliciel pour les élections et des mesures de contrôle qui seront mises en place.

9.1.3.2 VOTE SOUS LA CONTRAINTE ET ACHAT DE VOTES (INTÉGRITÉ DES VOTES ET EXACTITUDE DES RÉSULTATS)

Un particulier ou une organisation pourrait corrompre un votant ou le contraindre à voter pour un candidat précis par les moyens suivants :

- le vote est supervisé par la personne qui exerce la contrainte;
- le votant est en mesure, et peut donc être contraint, de montrer une preuve de son choix sur le bulletin de vote.

Menace 1 : Le votant pourrait exprimer un suffrage sous la surveillance d'une personne qui achète des votes ou exerce de la contrainte.

Probabilité : FAIBLE

Le fait de corrompre ou de contraindre un votant est possible, mais ce n'est pas courant dans des démocraties bien établies.

Impact : ÉLEVÉ

Quiconque achète des votes ou fait voter sous la contrainte pourrait modifier l'exactitude des résultats.

Atténuation :

- Le système doit produire des accusés de réception de vote qui ne permettent pas aux votants de prouver à un tiers pour qui ils ont voté (2.1.13.a).
- Le système doit empêcher quiconque, même les gestionnaires et les vérificateurs protégés, d'établir une corrélation entre les votes et les votants (2.1.13.b).

Risque : MOYEN

Il est possible de corrompre ou de contraindre un votant dans tout scénario dans lequel le vote est effectué à distance, sans supervision de la part d'un membre du personnel de scrutin. Cette possibilité est commune à tout système de vote à distance.

Il est à noter que les systèmes de vote à distance permettent de mettre en œuvre des mesures uniques pour atténuer ce risque : permettre aux votants de voter plusieurs fois, et de dépouiller seulement le dernier vote déposé.

Menace 2 : Un votant peut montrer ses options de vote à une personne qui achète des votes ou fait voter sous la contrainte.

Complexité / Probabilité : FAIBLE

il est possible mais non fréquent dans les démocraties bien établies d'acheter le vote d'une personne ou de la contraindre à voter avec une intention précise.

Impact : ÉLEVÉ

Quiconque achète des votes ou fait voter sous la contrainte pourrait modifier l'exactitude des résultats.

Atténuation :

- Le système doit produire des accusés de réception de vote qui ne permettent pas aux votants de prouver à un tiers pour qui ils ont voté (2.1.13.a).
- L'accusé de réception du vote doit protéger le secret du vote (c.-à-d. que l'on ne devrait jamais pouvoir déduire les options de vote retenues) (2.1.14.b).
- Le système doit empêcher quiconque, même les gestionnaires et les vérificateurs protégés, d'établir une corrélation entre les votes et les votants (2.1.13.b).

Risque : TRÈS FAIBLE

Comme l'accusé de réception du vote ne renferme pas de renseignements concernant les options de vote retenues, le votant ne serait pas en mesure de montrer son choix.

9.1.3.3 MODIFICATION DU VOTE (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Le contenu du vote pourrait être changé pour modifier les résultats de l'élection en ayant recours aux moyens suivants :

- en installant un logiciel malveillant sur les téléphones de vote;
- en interceptant le trafic entre le téléphone et le serveur de l'élection.

Menace 1 : Un logiciel malveillant utilisé dans les terminaux de votation peut modifier les options de vote retenues par les votants.

Complexité / Probabilité : TRÈS COMPLEXE

Il faudra posséder des compétences techniques très poussées et déployer beaucoup d'efforts pour installer un logiciel malveillant (qui n'est pas si répandu) dans les appareils téléphoniques pour accéder aux options de vote et les archiver. À l'heure actuelle, seuls certains téléphones mobiles sont visés par une quantité de maliciels, et affectent seulement des modes de scrutin basés sur des données, et non sur la voix.

Impact : ÉLEVÉ

Des bulletins de vote pourraient être modifiés.

Atténuation :

- *Vote sur site par téléphone* : le fournisseur de service doit décrire ses besoins en matériel, périphériques d'accessibilité, logiciel COTS, réseautage et dispositifs de sécurité pour assurer la disponibilité et la performance nécessaires. fournir des estimations pour les éléments de sauvegarde (2.3.5.b).

- *Vote sur site par téléphone* : le fournisseur de service est chargé de déployer le logiciel requis en plus du système d'exploitation, et de la configuration et du renforcement du système d'exploitation, et de la configuration des périphériques d'accessibilité (2.2.5.d).
- *Vote à distance par téléphone* : l'évaluation du risque qui a été effectuée a posé comme hypothèses que les téléphones personnels sont des téléphones courants non branchés à des sources de maliciel.

Risque : TRÈS FAIBLE

Le niveau de risque résiduel sera très faible en raison de la complexité du piratage téléphonique par maliciel pour les élections et des mesures de contrôle qui seront mises en place.

Menace 2 : Un pirate externe pourrait intercepter les communications entre le terminal de votation et le serveur de l'élection, et modifier les options de vote d'un vote.

Complexité / Probabilité : MOYENNE

L'interception de voies de communications téléphoniques n'est pas une tâche négligeable : elle nécessite une connaissance appropriée, des outils particuliers et un point d'accès précis pour surveiller le réseau téléphonique. Toutefois, les communications entre le RVI et les serveurs de l'élection sécurisés sont un peu plus faciles à intercepter.

Impact : ÉLEVÉ

Des bulletins de vote pourraient être modifiés.

Atténuation :

- Il n'y a pas de contrôles de sécurité assez rigoureux pour garantir l'intégrité du vote en transit, lorsque le vote est déposé par téléphone. Les mesures d'atténuation disponibles comprennent la réalisation de vérifications au sujet de l'infrastructure VRI et le déploiement de procédures adéquates devant être suivies par les opérateurs VRI et les administrateurs de système.

Risque : ÉLEVÉ

Le vote ne peut être protégé efficacement pour assurer son intégrité ou son authenticité (signature numérique) tant qu'un serveur de l'élection ne l'a pas reçu, car le terminal du téléphone ne permet pas cette opération; il faut donc faire confiance aux administrateurs VRI. Par conséquent, le niveau de risque résiduel sera élevé.

9.1.3.4 SUPPRESSION DU VOTE (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Un pirate pourrait tenter de supprimer des votes valides en interceptant les bulletins de vote et en les empêchant de se rendre aux serveurs de l'élection.

Menace 1 : Un pirate externe pourrait intercepter le vote une fois qu'il a quitté le téléphone de vote ou le système RVI et l'empêcher d'atteindre avec succès le serveur de l'élection, tout en laissant croire au votant que le bulletin de vote a été déposé avec succès.

Complexité / Probabilité : MOYENNE

L'interception de voies de communication n'est pas une tâche négligeable : elle nécessite une connaissance appropriée et des outils particuliers.

Impact : ÉLEVÉ

Des bulletins de vote pourraient être supprimés.

Atténuation :

- Le système doit fournir aux votants un accusé de réception une fois qu'ils ont déposé leur vote. Cet accusé de réception leur permettra de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de dépouillement (1.2.6.a).
- Le système doit permettre aux votants de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de compilation au moyen d'un accusé de réception. (2.1.8.a).

Risque : FAIBLE

Comme le vote sera confirmé au moyen d'un accusé de réception (vérifiable une fois la période de vote terminée), le risque résiduel de supprimer un vote en transit sera faible.

9.1.3.5 INCERTITUDE DU VOTANT QUANT AU BULLETIN DE VOTE DÉPOSÉ (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Si un votant ne dispose pas d'une façon de vérifier la réception et le dépouillement corrects de son vote, il pourrait commencer à éprouver de l'incertitude quant au processus électoral.

Menace 1 : Le votant pourrait douter que son vote a été archivé dans l'urne.

Complexité / Probabilité : ÉLEVÉE

Il est fort possible qu'un votant soit incertain que son vote téléphonique a été bien archivé dans l'urne.

Impact : ÉLEVÉ

Les élections pourraient perdre de la crédibilité.

Atténuation :

- Le système doit fournir aux votants un accusé de réception une fois qu'ils ont déposé leur vote. Cet accusé de réception leur permettra de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de dépouillement (1.2.6.a).
- Le système doit permettre aux votants de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de compilation au moyen d'un accusé de réception (2.1.8.a).
- Le processus de vérification doit permettre de détecter les accusés de réception manipulés ou contrefaits pour empêcher les déclarations frauduleuses des votants (2.1.8.c).

Risque : FAIBLE

Comme le votant aura un accusé de réception et la possibilité de s'assurer que son bulletin de vote a été dénombré, le niveau de risque résiduel sera faible.

Menace 2 : Le votant pourrait avoir l'impression que son vote n'a pas été déposé adéquatement.

Probabilité : ÉLEVÉE

Il est fort possible qu'un votant soit incertain que son vote par téléphone a été transmis correctement et bien archivé dans l'urne.

Impact : ÉLEVÉ

Les élections pourraient ne pas avoir assez de crédibilité.

Atténuation :

- Le système doit fournir aux votants un accusé de réception une fois qu'ils ont déposé leur vote. Cet accusé de réception leur permettra de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de dépouillement (1.2.6.a).
- Le système doit permettre aux votants de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de compilation au moyen d'un accusé de réception. (2.1.8.a).
- Le processus de vérification doit permettre de détecter les accusés de réception manipulés ou contrefaits pour empêcher les déclarations frauduleuses des votants (2.1.8.c).

Risque : FAIBLE

Comme le votant aura un accusé de réception et pourra s'assurer que son bulletin de vote a été pris en compte dans le résultat, le niveau de risque résiduel sera faible.

9.1.4 ARCHIVAGE DE VOTE ET GESTION DE L'URNE

Le processus d'archivage de vote et de gestion de l'urne comprend les catégories de risque suivantes :

- mise en péril de la confidentialité,
- publication non autorisée des résultats intermédiaires,
- remplissage de bulletins de vote,
- modification de vote,
- suppression de vote,
- refus de service (boycott de l'élection).

9.1.4.1 MISE EN PÉRIL DE LA CONFIDENTIALITÉ DU VOTANT (VIE PRIVÉE ET CONFIDENTIALITÉ DU VOTANT)

Un pirate à l'interne pourrait violer la vie privée du votant en accédant directement aux serveurs de l'élection et en reliant le votant et son choix de vote.

Menace 1 : Un administrateur de système ayant accès aux serveurs de l'élection serait en mesure d'accéder à toute l'urne qui contient les votes déposés.

Complexité / Probabilité : FACILE

Un administrateur de système possédant les autorisations appropriées pourrait accéder aisément à la base de données qui archive les bulletins de vote.

Impact : TRÈS ÉLEVÉ

Quiconque accède à l'urne pourrait prendre connaissance de tous les bulletins de vote déposés.

Atténuation :

- Le système doit garantir qu'un bulletin de vote déposé demeure secret devant les tiers, dont les administrateurs de système et les pirates éventuels qui franchissent les mesures de sécurité traditionnelles qui protègent la plateforme de vote (2.1.4.a).
- Le système doit garantir que seul le conseil de gestion du vote en réseau peut déchiffrer les votes, après l'élection, idéalement dans un milieu isolé (p.ex., sans être branché à un réseau de communication) (2.1.1.b).
- Le système doit garantir que la clé nécessaire pour déchiffrer les votes n'est pas disponible pendant le processus de vote jusqu'à ce que le conseil de gestion du vote en réseau la retire/la reconstitue (2.1.2.b).
- Le système doit garantir qu'au moins une majorité établie au préalable des membres du conseil de gestion du vote en réseau est nécessaire pour retirer la clé de déchiffrement de l'élection (2.1.2.c).
- Le système doit garantir que les votes sont chiffrés d'une façon que seul le conseil de gestion du vote en réseau peut déchiffrer (2.1.2.a, 2.1.4.c).
- Le système doit protéger les votes (p. ex. par le chiffrement) dans le terminal de votation du votant avant qu'ils soient transmis au serveur de l'élection (2.1.1.a, 2.1.4.b).
- Le système doit garantir que deux votes différents dont le contenu est identique présentent des formats de chiffrement différents (2.1.2.e).

Risque : TRÈS FAIBLE

Comme le vote sera archivé sous forme chiffrée sans possibilité que l'administrateur de système accède à la clé de déchiffrement, le niveau de risque résiduel sera très faible.

9.1.4.2 PUBLICATION DE RÉSULTATS INTERMÉDIAIRES NON AUTORISÉS (VIE PRIVÉE ET CONFIDENTIALITÉ DU VOTANT)

Les résultats intermédiaires pourraient être divulgués avant la clôture de l'élection, ce qui influencerait les votants qui n'ont pas encore exercé leur droit de vote. Cette divulgation pourrait survenir par les moyens suivants :

- par l'accès aux serveurs de l'élection;
- à la suite de l'interception des votes en transit dans l'infrastructure de vote en réseau;
- à la suite de l'interception des votes en transit dans les serveurs vri;
- par la compilation des résultats avant la clôture du scrutin.

Menace 1 : quiconque ayant accès aux serveurs de l'élection pourrait calculer et publier les résultats intermédiaires.

Complexité / Probabilité : FACILE

Un administrateur de système possédant les autorisations appropriées peut facilement avoir accès à la base de données qui archive les bulletins de vote.

Impact : ÉLEVÉ

Si une personne calcule et publie les résultats intermédiaires de l'élection, cette personne pourrait influencer les votants qui n'ont pas encore exercé leur droit de vote, ce qui modifierait le résultat final de l'élection.

Atténuation :

- Le système doit garantir que deux votes différents dont le contenu est identique présentent des formats de chiffrement différents (2.1.2.e).
- Le système doit garantir qu'un bulletin de vote déposé demeure secret devant les tiers, dont les administrateurs de système et les pirates éventuels qui franchissent les mesures de sécurité traditionnelles qui protègent la plateforme de vote (2.1.4.a).
- Le système doit garantir que seul le conseil de gestion du vote en réseau peut déchiffrer les votes, après l'élection, idéalement dans un milieu isolé (p.ex., sans être branché à un réseau de communication) (2.1.1.b).
- Le système doit garantir que la clé nécessaire pour déchiffrer les votes n'est pas disponible pendant le processus de vote jusqu'à ce que le conseil de gestion du vote en réseau la retire/la reconstitue (2.1.2.b).
- Le système doit garantir qu'au moins une majorité établie au préalable des membres du conseil de gestion du vote en réseau est nécessaire pour retirer la clé de déchiffrement de l'élection (2.1.2.c).
- Le système doit garantir que les votes sont chiffrés d'une façon que seul le conseil de gestion du vote en réseau peut déchiffrer (2.1.2.a, 2.1.4.c).
- Le système doit protéger les votes (p. ex. par le chiffrement) dans le terminal de votation du votant avant qu'ils soient transmis au serveur de l'élection (2.1.1.a, 2.1.4.b).

Risque : TRÈS FAIBLE

Comme le vote sera chiffré de la sélection au processus de déchiffrement, qui sera exécuté à la fin de l'élection, le niveau de risque résiduel sera très faible.

Menace 2 : quiconque ayant accès à la composante de l'infrastructure intermédiaire dans les serveurs de l'élection en réseau aurait accès aux votes en transit, et serait en mesure de calculer et de publier des résultats intermédiaires.

Complexité / Probabilité : FACILE

Un administrateur de système possédant les autorisations appropriées pourrait facilement avoir accès à la base de données qui archive les bulletins de vote.

Impact : ÉLEVÉ

Si une personne calcule et publie les résultats intermédiaires de l'élection, cette personne pourrait influencer les votants qui n'ont pas encore exercé leur droit de vote, ce qui modifierait les résultats de l'élection.

Atténuation :

- Le système doit garantir que deux votes différents dont le contenu est identique présentent des formats de chiffrement différents (2.1.2.e).
- Le système doit garantir qu'un bulletin de vote déposé demeure secret devant les tiers, dont les administrateurs de système et les pirates éventuels qui franchissent les mesures de sécurité traditionnelles qui protègent la plateforme de vote (2.1.4.a).

- Le système doit garantir que seul le conseil de gestion du vote en réseau peut déchiffrer les votes, après l'élection, idéalement dans un milieu isolé (p.ex., sans être branché à un réseau de communication) (2.1.1.b).
- Le système doit garantir que la clé nécessaire pour déchiffrer les votes n'est pas disponible pendant le processus de vote jusqu'à ce que le conseil de gestion du vote en réseau la retire/la reconstitue (2.1.2.b).
- Le système doit garantir qu'au moins une majorité établie au préalable des membres du conseil de gestion du vote en réseau est nécessaire pour retirer la clé de déchiffrement de l'élection (2.1.2.c).
- Le système doit garantir que les votes sont chiffrés d'une façon que seul le conseil de gestion du vote en réseau peut déchiffrer (2.1.2.a, 2.1.4.c).
- le système doit protéger les votes (p. ex. par le chiffrement) dans le terminal de votation du votant avant qu'ils soient transmis au serveur de l'élection (2.1.1.a, 2.1.4.b).

Risque : TRÈS FAIBLE

Comme le vote sera chiffré de la sélection au processus de déchiffrement, qui sera exécuté à la fin de l'élection, le niveau de risque résiduel sera très faible.

Menace 3 : Quiconque a accès à une composante de l'infrastructure intermédiaire dans la plateforme vri aurait accès aux votes en transit, et serait en mesure de calculer et de publier des résultats intermédiaires.

Complexité / Probabilité : FACILE

Un administrateur de système possédant les autorisations appropriées pourrait facilement avoir accès à la base de données qui archive les bulletins de vote et intercepter les données non chiffrées en transit dans les serveurs.

Impact : ÉLEVÉ

Si une personne calcule et publie les résultats intermédiaires de l'élection, cette personne pourrait influencer les votants qui n'ont pas encore exercé leur droit de vote, ce qui modifierait le résultat final de l'élection.

Atténuation :

Le fournisseur de service sera chargé de déployer le logiciel requis en plus du système d'exploitation (dont les serveurs d'application, les bases de données, etc.), et sera chargé de la configuration et de la protection accrue du système d'exploitation (2.2.3.e).

- Il n'existe pas de mesure d'atténuation efficace qui permette d'éviter que les administrateurs VRI accèdent aux données en transit. Plusieurs procédures limitant l'accès au système doivent être mises en place pour rendre la concrétisation de ce risque plus complexe.

Risque : ÉLEVÉ

Quoique la plateforme VRI fera l'objet d'un processus de renforcement de sécurité, on estime qu'il n'y aura pas assez de mesures de contrôle efficaces pour garantir qu'un administrateur de plateforme VRI n'aura pas accès aux bulletins de vote déposés par les votants. Par conséquent, le niveau de risque résiduel demeurera élevé.

Menace 4 : Un responsable de l'élection pourrait effectuer le processus de compilation avant la fin de la période de vote et obtenir des résultats intermédiaires.

Complexité / Probabilité : FACILE

Un responsable de l'élection pourrait tenter facilement d'exécuter le processus de compilation avant la fin de la période de vote.

Impact : ÉLEVÉ

Si une personne calcule et publie les résultats intermédiaires de l'élection, cette personne pourrait influencer les votants qui n'ont pas encore exercé leur droit de vote, ce qui modifierait le résultat de l'élection.

Atténuation :

- Le système doit garantir que seul le conseil de gestion du vote en réseau peut déchiffrer les votes, après l'élection, idéalement dans un milieu isolé (p.ex., sans être branché à un réseau de communication) (2.1.1.b).
- Le système doit garantir que la clé nécessaire pour déchiffrer les votes n'est pas disponible pendant le processus de vote jusqu'à ce que le conseil de gestion du vote en réseau la retire/la reconstitue (2.1.2.b).
- Le système doit garantir qu'au moins une majorité établie au préalable des membres du conseil de gestion du vote en réseau est nécessaire pour retirer la clé de déchiffrement de l'élection (2.1.2.c).
- Le système doit garantir que les votes sont chiffrés d'une façon que seul le conseil de gestion du vote en réseau peut déchiffrer (2.1.2.a, 2.1.4.c).
- Le système a recours au conseil de gestion du vote en réseau pour déchiffrer les votes déposés (2.1.7.a).
- Le système utilise un schéma cryptographique à seuil des membres du conseil de gestion du vote en réseau pour extraire les clés permettant le déchiffrement des votes (2.1.7.b).
- Il doit être impossible pour un membre ou un certain nombre de membres sous le seuil d'extraire la clé de déchiffrement de l'élection (2.1.7.c).
- Le système doit prendre en charge le recours à des dispositifs inviolables (p. ex., des cartes à puce intelligentes protégées par un NIP) pour archiver l'information dont a besoin chaque membre du conseil de gestion du vote en réseau pour extraire la clé de déchiffrement de l'élection (2.1.7.d).
- Le seuil repose sur une méthode cryptographique (p. ex., le plan de partage secret) (2.1.7.e).
- La clé de déchiffrement est détruite par le schéma à seuil et n'existe pas tant qu'elle n'est pas reconstruite par les membres du conseil de gestion du vote en réseau à la fin de l'élection (2.1.7.f).

Risque : TRÈS FAIBLE

Comme le vote sera chiffré jusqu'au processus de déchiffrement, qui sera exécuté à la fin de l'élection par une majorité qualifiée, le niveau de risque résiduel sera très faible.

9.1.4.3 REMPLISSAGE DES URNES (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Un pirate peut tenter d'ajouter à l'urne des votes de votants qui n'ont pas participé au processus de vote en ayant recours aux moyens suivants :

- un travailleur en place malveillant pourrait insérer des votes directement dans la base de données;
- un pirate interne ou externe pourrait insérer des votes directement dans la base de données;
- une urne préparée pourrait être chargée dans le serveur de l'élection avant le début du scrutin.

Menace 1 : Quiconque ayant accès aux serveurs de l'élection et à l'urne pourrait tenter d'insérer des votes directement dans la base de données.

Complexité / Probabilité : FACILE

Un administrateur de système possédant les autorisations appropriées peut facilement avoir accès à la base de données qui archive les bulletins de vote.

Impact : TRÈS ÉLEVÉ

Quiconque a accès au serveur de l'élection aurait directement accès à la base de données pour insérer un nouveau vote, ce qui modifierait le résultat de l'élection.

Atténuation :

- Le système doit empêcher l'ajout de votes contrefaits par des utilisateurs externes et des administrateurs du système (2.1.6.b, 2.1.5.d).
- Le système doit, à des fins de vérification, permettre de retracer avec exactitude les processus qui ont mené au dépôt et à l'archivage d'un vote dans une urne (2.1.6.c).
- Une cryptographie solide, qui a notamment recours à des signatures numériques, devrait protéger l'intégrité du vote (2.1.5.e).
- Le système doit permettre de vérifier l'intégrité et l'identité du service qui a géré l'urne avant d'entreprendre le processus de déchiffrement et de compilation (2.1.6.a).

Risque : TRÈS FAIBLE

Comme l'intégrité de l'urne électronique sera protégée et les votes porteront une signature numérique, le niveau de risque résiduel sera très faible.

Menace 2 : Un pirate interne ou externe pourrait déposer des votes à partir d'un serveur intermédiaire ou d'une autre composante du système de vote (évitant ainsi les filtres qui empêchent ce genre de comportement de la part des votants).

Complexité / Probabilité : MOYENNE

Il n'est pas négligeable d'avoir accès aux serveurs intermédiaires. dans ce cas précis, les attaques internes ne sont pas prises en compte, car la description de l'attaque précédente englobe de telles attaques.

Impact : ÉLEVÉ

Quiconque a accès à un serveur intermédiaire pourrait modifier l'exactitude des résultats en déposant des votes additionnels.

Atténuation :

- Le système doit empêcher l'ajout de votes contrefaits par des utilisateurs externes et des administrateurs du système (2.1.6.b, 2.1.5.d).
- Le système doit, à des fins de vérification, permettre de retracer avec exactitude les processus qui ont mené au dépôt et à l'archivage d'un vote dans une urne (2.1.6.c).
- Le système doit permettre de vérifier l'intégrité et l'identité du service qui a géré l'urne avant d'entreprendre le processus de déchiffrement et de compilation (2.1.6.a).
- Une cryptographie solide, qui a notamment recours à des signatures numériques, devrait protéger l'intégrité du vote (2.1.5.e).

Risque : TRÈS FAIBLE

Comme l'authenticité des votes archivés dans l'urne électronique sera garantie, le niveau de risque résiduel sera très faible.

Menace 3 : Avant le début de l'élection, un travailleur en place malveillant pourrait charger une urne électronique déjà préparée dans les serveurs de l'élection.

Complexité / Probabilité : FACILE

Un administrateur de système possédant les autorisations appropriées peut facilement avoir accès à la base de données qui archive les bulletins de vote et y intégrer une urne électronique préparée qui contient déjà des votes.

Impact : TRÈS ÉLEVÉ

Quiconque a accès aux serveurs de l'élection aurait accès à toute l'urne pour insérer le contenu d'une urne qui renferme des votes contrefaits.

Atténuation :

- Le système doit protéger l'intégrité et l'authenticité de l'information sur l'élection qui est utilisée pour configurer la plateforme de vote (1.1.1.b).
- Le système doit permettre de vérifier l'intégrité et l'identité du service qui a géré l'urne avant d'entreprendre le processus de déchiffrement et de compilation (2.1.6.a).
- Le système doit empêcher l'ajout de votes contrefaits par des utilisateurs externes et des administrateurs du système (2.1.6.b, 2.1.5.d).
- Le système doit, à des fins de vérification, permettre de retracer avec exactitude les processus qui ont mené au dépôt et à l'archivage d'un vote dans une urne (2.1.6.c).
- Une cryptographie solide, qui a notamment recours à des signatures numériques, devrait protéger l'intégrité du vote (2.1.5.e).

Risque : TRÈS FAIBLE

Comme l'intégrité et l'authenticité de l'urne électronique seront protégées, et que les votes doivent porter la signature numérique des votants, le niveau de risque résiduel sera très faible.

9.1.4.4 MODIFICATION DU VOTE (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Le contenu du vote pourrait être changé de manière à modifier les résultats de l'élection.

Menace 1 : Un administrateur de système ou un pirate externe pourrait avoir directement accès à l'urne et modifier le contenu d'un vote valide.

Complexité / Probabilité : FACILE

Un administrateur de système possédant les autorisations appropriées pourrait facilement avoir accès à la base de données qui archive les bulletins de vote.

Impact : TRÈS ÉLEVÉ

Quiconque a accès à toute l'urne pourrait modifier l'ensemble des votes, ce qui modifierait sérieusement le résultat de l'élection.

Atténuation :

- Une cryptographie solide, qui a notamment recours à des signatures numériques, devrait protéger l'intégrité du vote (2.1.5.e).
- Le système doit, à des fins de vérification, permettre de retracer avec exactitude les processus qui ont mené au dépôt et à l'archivage d'un vote dans une urne (2.1.6.c).
- Le système doit protéger l'intégrité de chaque vote déposé pendant tout le processus électoral (2.1.5.a).
- Le système doit protéger par des moyens cryptographiques la confidentialité et l'intégrité du vote déposé, ainsi que l'identité du votant, afin que le vote ne puisse être altéré pendant son transport ou son archivage (1.2.5.b).
- Les votes déposés doivent être protégés contre les attaques externes et internes (p. ex. par les administrateurs de système) en ayant recours à des mesures cryptographiques adéquates pouvant être démontrées devant un expert en matière de sécurité ou un vérificateur (1.2.5.d).

Risque : TRÈS FAIBLE

Comme l'intégrité et l'authenticité de l'urne électronique seront protégées, et que les votes doivent porter la signature numérique des votants, le niveau de risque résiduel sera très faible.

9.1.4.5 SUPPRESSION DE VOTE (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Un pirate pourrait tenter de supprimer des votes valides de l'urne.

Menace 1 : un administrateur de système ou un pirate externe pourrait avoir directement accès à l'urne et supprimer un vote valide.

Complexité / Probabilité : FACILE

Un administrateur de système possédant les autorisations appropriées peut facilement avoir accès à la base de données qui archive les bulletins de vote.

Impact : TRÈS ÉLEVÉ

Plusieurs bulletins de vote pourraient être supprimés, ce qui affecterait l'exactitude du résultat de l'élection.

Atténuation :

- Le système doit mettre en œuvre des mesures adéquates pour détecter les anomalies au cours du processus de vote (2.1.6.d).
- Le système doit, à des fins de vérification, permettre de retracer avec exactitude les processus qui ont mené au dépôt et à l'archivage d'un vote dans une urne (2.1.6.c).
- Le système doit permettre de vérifier l'intégrité et l'identité du service qui a géré l'urne avant d'entreprendre le processus de déchiffrement et de compilation (2.1.6.a).
- Le système doit fournir aux votants un accusé de réception une fois qu'ils ont déposé leur vote. Cet accusé de réception leur permettra de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de dépouillement (1.2.6.a).
- Le système doit permettre aux votants de s'assurer de la présence de leur vote pendant le processus de déchiffrement et de compilation au moyen d'un accusé de réception (2.1.8.a).

Risque : TRÈS FAIBLE

Comme l'intégrité de l'urne électronique sera protégée, le niveau de risque résiduel sera très faible.

9.1.4.6 BOYCOTT DE L'ÉLECTION – REFUS DE SERVICE (DISPONIBILITÉ DES SYSTÈMES ÉLECTORAUX)

Un pirate pourrait perturber la disponibilité du mode de scrutin par une attaque entraînant un refus de service en inondant le système de demandes.

Menace 1 : Le système de vote pourrait être inondé de fausses demandes de voter pour surcharger le système et empêcher que des votes valides soient reçus.

Complexité / Probabilité : FACILE

Des compétences techniques de base seraient nécessaires pour inonder le système de vote de demandes de voter simulées. Ces demandes pourraient prendre la forme de demandes de connexion, de chargements de page, ou d'autres demandes qui ont recours aux ressources du serveur.

Impact : ÉLEVÉ

Le système de vote pourrait être indisponible à des moments cruciaux.

Atténuation :

- Le système de vote doit fournir des outils de surveillance qui détectent les anomalies au cours du processus de vote (1.2.8.a).
- Le système de vote doit être disponible 99,95 % du temps au cours de la période de vote (2.2.1.a).

- Le système de vote doit pouvoir prendre en charge simultanément assez de votants qui votent par ordinateur et, en parallèle, assez de votants qui votent par téléphone. (2.2.1.b). Le nombre de lignes sera fonction du nombre de votants prévus. S'il y a deux téléphones par centre de scrutin, au moins vingt lignes devraient être disponibles.
- Les terminaux de votation situés dans les bureaux de scrutin doivent pouvoir fonctionner durant toute la période de vote (2.2.1.c).
- Le système devrait être en mesure de prendre des élections en charge pour des dizaines de millions de votants facilement et de manière économique (2.4.1.a).
- Le système doit permettre d'ajouter de nouvelles composantes sans avoir à mettre fin au service, p. ex. pour prendre en charge un plus grand nombre de votants (2.4.1.b).
- Le système doit pouvoir fonctionner parallèlement dans deux environnements différents : sur site (à partir des bureaux de vote) et à distance (de n'importe où) (2.4.2.d).
- Le fournisseur de service est chargé de déployer le logiciel requis et le système d'exploitation (y compris les serveurs de l'application, les bases de données, etc.), et de configurer et renforcer le système d'exploitation (2.2.2.d).

Risque : FAIBLE

Comme plusieurs mesures de contrôle permettront de détecter et de faire cesser une attaque entraînant un refus de service, et pourvu que le système de vote soit disponible pendant au moins six jours, le niveau de risque résiduel sera faible.

Menace 2 : Les serveurs de l'élection pourraient être inondés de demandes malveillantes pour provoquer une défaillance du serveur et empêcher la réception de votes du réseau.

Complexité / Probabilité : FACILE

Des compétences techniques de base seront nécessaires pour inonder les serveurs de l'élection de demandes malveillantes.

Impact : ÉLEVÉ

Le système de vote pourrait être indisponible à des moments cruciaux.

Atténuation :

- Le fournisseur de service est chargé de déployer le logiciel requis et le système d'exploitation (y compris les serveurs de l'application, les bases de données, etc.), et de configurer et renforcer le système d'exploitation (2.2.2.d).
- Le système de vote doit fournir des outils de surveillance qui détectent les anomalies au cours du processus de vote (1.2.8.a).
- Le système de vote doit être disponible 99,95 % du temps au cours de la période de vote (2.2.1.a).

Risque : faible

Comme plusieurs mesures de contrôle permettront de détecter et de faire cesser une attaque entraînant un refus de service, et pourvu que le système de vote soit disponible pendant plusieurs jours, le niveau de risque résiduel sera faible.

9.1.5 COMPILATION

Le processus de compilation est exposé à plusieurs risques :

- mise en péril de la confidentialité
- remplissage des urnes
- modification de votes
- suppression de votes
- modification des résultats du votant.

9.1.5.1 MISE EN PÉRIL DE LA CONFIDENTIALITÉ DU VOTANT (VIE PRIVÉE ET CONFIDENTIALITÉ DU VOTANT)

Un pirate pourrait violer la vie privée du votant et établir une corrélation entre le votant et les options de vote retenues.

Menace 1 : Un responsable de l'élection pourrait avoir accès aux votes au cours du processus de compilation et identifier les options de vote de chaque votant.

Complexité / Probabilité : MOYENNE

Un responsable de l'élection pourrait difficilement avoir un accès direct au contenu du vote durant le processus de compilation s'il a lieu devant de nombreuses parties prenantes.

Impact : ÉLEVÉ

Toute personne ayant accès au processus de compilation prendrait connaissance de tous les votes.

Atténuation :

- Le processus de déchiffrement et de dépouillement doit être exécuté dans un lieu isolé qui n'est pas branché à internet (1.3.2.a).
- Le processus de déchiffrement et de compilation doit faire en sorte qu'il est impossible d'établir une corrélation entre l'ordre des bulletins de vote déchiffrés et l'ordre dans lequel ils ont été déposés et, en conséquence, doit empêcher tout lien entre les bulletins de vote déchiffrés et les votants (p. ex. En ayant recours à un procédé de mélange) (1.3.2.g).
- Le système doit garantir qu'il est impossible d'établir une corrélation entre l'ordre dans lequel les votes ont été déchiffrés et l'ordre dans lequel ils ont été déposés (2.1.2.d).

Risque : TRÈS FAIBLE

Comme il existe un processus qui assure l'impossibilité d'établir une corrélation entre les bulletins de vote déposés et les votants, le niveau de risque résiduel sera très faible.

9.1.5.2 REMPLISSAGE DE L'URNE (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Au cours du processus de compilation, un travailleur en place malveillant pourrait tenter d'ajouter des votes de votants qui n'avaient pas pris part au processus de vote.

Menace 1 : Un responsable de l'élection pourrait ajouter des votes contrefaits au système pendant le processus de compilation.

Complexité / Probabilité : MOYENNE

Il n'est nullement banal pour un responsable de l'élection d'ajouter des votes contrefaits durant le processus de compilation, à la condition que ce soit fait devant de nombreuses parties prenantes. Le responsable de l'élection devrait également posséder certaines connaissances techniques de pointe pour ajouter des bulletins de vote contrefaits dans un système de vote en réseau.

Impact : TRÈS ÉLEVÉ

Quiconque ajoute des votes contrefaits pourrait modifier l'exactitude des résultats.

Atténuation :

- Le processus de déchiffrement et de dépouillement doit être exécuté dans un lieu isolé qui n'est pas branché à internet (1.3.2.a).
- Le système doit permettre de vérifier l'intégrité et l'identité du service qui a géré l'urne avant d'entreprendre le processus de déchiffrement et de compilation (2.1.6.a).
- Le système doit empêcher l'ajout de votes contrefaits par des utilisateurs externes et des administrateurs du système (2.1.6.b, 2.1.5.d).
- Le système doit permettre à des vérificateurs indépendants ou au conseil de gestion du vote en réseau d'exécuter de nouveaux processus de déchiffrement et de compilation au besoin (1.3.5.a).
- Le système doit permettre à des vérificateurs indépendants d'effectuer des recomptages parallèles à la liste certifiée des bulletins de vote déchiffrés (1.3.5.b).
- Le système doit permettre à des vérificateurs indépendants de vérifier et de certifier l'intégrité et l'authenticité des composantes du système utilisées pour traiter les urnes (1.3.5.c).

Risque : TRÈS FAIBLE

Comme l'urne électronique sera protégée et isolée, et que les opérations y seront faites après coup, le niveau de risque résiduel sera très faible.

9.1.5.3 MODIFICATION DU VOTE (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Le contenu du vote pourrait être changé de manière à modifier les résultats de l'élection.

Menace 1 : Au cours du processus de compilation, un responsable de l'élection pourrait remplacer des votes valides par des votes contrefaits, voire remplacer toute l'urne par une urne contrefaite.

Complexité / Probabilité : MOYENNE

Un responsable de l'élection pourrait difficilement ajouter des votes contrefaits, voire remplacer l'urne complète pendant le processus de compilation, car celui-ci est exécuté devant de nombreuses parties prenantes. Le responsable de l'élection devrait également posséder des connaissances techniques de pointe pour ajouter des bulletins de vote contrefaits dans un système de vote en réseau.

Impact : TRÈS ÉLEVÉ

Quiconque a accès à l'ensemble de l'urne pourrait modifier l'un ou l'autre ou la totalité des votes.

Atténuation :

- le processus de déchiffrement et de dépouillement doit être exécuté dans un lieu isolé qui n'est pas branché à internet (1.3.2.a).
- le système doit permettre de vérifier l'intégrité et l'identité du service qui a géré l'urne avant d'entreprendre le processus de déchiffrement et de compilation (2.1.6.a).
- le système doit permettre à des vérificateurs indépendants ou au conseil de gestion du vote en réseau d'exécuter de nouveaux processus de déchiffrement et de compilation au besoin (1.3.5.a).
- le système doit permettre à des vérificateurs indépendants d'effectuer des recomptages parallèles à la liste certifiée des bulletins de vote déchiffrés (1.3.5.b).
- le système doit permettre à des vérificateurs indépendants de vérifier et de certifier l'intégrité et l'authenticité des composantes du système utilisées pour traiter les urnes (1.3.5.c).

Risque : TRÈS FAIBLE

Comme l'urne électronique sera protégée et isolée, et que les opérations y seront faites après coup, le niveau de risque résiduel sera très faible.

9.1.5.4 SUPPRESSION DE VOTE (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Un travailleur en place malveillant pourrait tenter de supprimer des votes valides de l'urne.

Menace 1 : Pendant le processus de compilation, un responsable de l'élection pourrait supprimer des votes du système.

Complexité / Probabilité : MOYENNE

Un responsable de l'élection pourrait difficilement supprimer des votes pendant le processus de compilation, car celui-ci est exécuté devant de nombreuses parties prenantes. Le responsable de l'élection devrait également posséder des connaissances techniques de pointe pour supprimer des bulletins de vote dans un système de vote en réseau.

Impact : TRÈS ÉLEVÉ

Quiconque supprime des votes contrefaits pourrait modifier l'exactitude des résultats.

Atténuation :

- Le processus de déchiffrement et de dépouillement doit être exécuté dans un lieu isolé qui n'est pas branché à internet (1.3.2.a).
- Le système doit mettre en œuvre des mesures adéquates pour détecter les anomalies au cours du processus de vote (2.1.6.d).
- Le système doit fournir aux votants un accusé de réception une fois qu'ils ont déposé leur vote. Cet accusé de réception leur permettra de vérifier que leur vote était présent pendant le processus de déchiffrement et de dépouillement (1.2.6.a).

- Le système doit permettre de vérifier l'intégrité et l'identité du service qui a géré l'urne avant d'entreprendre le processus de déchiffrement et de compilation (2.1.6.a).
- Le système doit permettre à des vérificateurs indépendants ou au conseil de gestion du vote en réseau d'exécuter de nouveaux processus de déchiffrement et de compilation au besoin (1.3.5.a).
- Le système doit permettre à des vérificateurs indépendants d'effectuer des recomptages parallèles à la liste certifiée des bulletins de vote déchiffrés (1.3.5.b).
- Le système doit permettre à des vérificateurs indépendants de vérifier et de certifier l'intégrité et l'authenticité des composantes du système utilisées pour traiter les urnes (1.3.5.c).

Risque : TRÈS FAIBLE

Comme l'urne électronique sera protégée et isolée, et que les opérations y seront faites après coup, le niveau de risque résiduel sera très faible.

9.1.5.5 MODIFICATION DES RÉSULTATS DU SCRUTIN (INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS)

Les résultats de l'élection peuvent être modifiés sans modifier les votes ou l'urne, mais plutôt en manipulant les processus de compilation ou de dépouillement.

Menace 1 : Un responsable de l'élection pourrait modifier les résultats du vote pendant le processus de vote.

Complexité / Probabilité : MOYENNE

Un responsable de l'élection pourrait difficilement modifier le processus de dépouillement, car celui-ci est exécuté devant de nombreuses parties prenantes.

Impact : TRÈS ÉLEVÉ

Les résultats de l'élection pourraient être mis en péril.

Atténuation :

- le processus de déchiffrement et de dépouillement doit être exécuté dans un lieu isolé qui n'est pas branché à internet (1.3.2.a).
- le système doit permettre à des vérificateurs indépendants ou au conseil de gestion du vote en réseau d'exécuter de nouveaux processus de déchiffrement et de compilation au besoin (1.3.5.a).
- le système doit permettre à des vérificateurs indépendants d'effectuer des recomptages parallèles à la liste certifiée des bulletins de vote déchiffrés (1.3.5.b).
- le système doit permettre à des vérificateurs indépendants de vérifier et de certifier l'intégrité et l'authenticité des composantes du système utilisées pour traiter les urnes (1.3.5.c).
- l'information transférée au SGE d'Élections Ontario doit être protégée pour assurer son intégrité et son authenticité (1.3.3.c).

Risque : TRÈS FAIBLE

Comme le processus de dépouillement sera exécuté dans un environnement isolé, l'intégrité de l'urne électronique sera contrôlée et les résultats de la compilation seront protégés, le niveau de risque résiduel sera très faible.

Menace 2 : L'application de vote pourrait modifier les résultats du scrutin pendant le processus de dépouillement.

Complexité / Probabilité : MOYENNE

Un programmeur ayant accès à l'application de vote pourrait difficilement modifier le logiciel pour changer les résultats du scrutin en passant inaperçu, compte tenu du fait que le code devrait avoir fait l'objet d'une vérification avant l'élection et que le processus de dépouillement est exécuté dans un environnement isolé devant plusieurs parties prenantes.

Impact : TRÈS ÉLEVÉ

Les résultats de l'élection pourraient être mis en péril.

Atténuation :

- Les vérificateurs doivent avoir accès au code source du système si Élections Ontario le demande (1.4.2.a).
- Le système doit permettre de vérifier l'intégrité et l'identité du service qui a géré l'urne avant d'entreprendre le processus de déchiffrement et de compilation (2.1.6.a).
- Le système doit permettre à des vérificateurs indépendants ou au conseil de gestion du vote en réseau d'exécuter de nouveaux processus de déchiffrement et de compilation au besoin (1.3.5.a).
- Le système doit permettre à des vérificateurs indépendants d'effectuer des recomptages parallèles à la liste certifiée des bulletins de vote déchiffrés (1.3.5.b).
- Le système doit permettre à des vérificateurs indépendants de vérifier et de certifier l'intégrité et l'authenticité des composantes du système utilisées pour traiter les urnes (1.3.5.c).

Risque : FAIBLE

Outre le processus de certification / de vérification de logiciel, des processus de dépouillement indépendants devraient être exécutés pour vérifier les résultats obtenus.

Menace 3 : Un pirate (externe ou interne) pourrait modifier les résultats de l'élection après le processus de dépouillement.

Complexité / Probabilité : MOYENNE

Il n'est pas banal de modifier les résultats de l'élection après le processus de dépouillement, compte tenu du fait que ce processus est exécuté dans un environnement isolé devant plusieurs parties prenantes.

Impact : TRÈS ÉLEVÉ

Les résultats de l'élection pourraient être mis en péril.

Atténuation :

- Le processus de déchiffrement et de dépouillement doit être exécuté dans un lieu isolé qui n'est pas branché à internet (1.3.2.a).

- Les composantes du système de vote utilisé pour configurer l'élection et pour déchiffrer et compiler les bulletins de vote doivent fonctionner dans un environnement isolé composé d'un ou plusieurs serveurs/ordinateurs (2.2.4.a).
- L'information transférée au SGE d'Élections Ontario doit être protégée pour assurer son intégrité et son authenticité (1.3.3.c).
- Le système doit permettre à des vérificateurs indépendants ou au conseil de gestion du vote en réseau d'exécuter de nouveaux processus de déchiffrement et de compilation au besoin (1.3.5.a).
- Le système doit permettre à des vérificateurs indépendants d'effectuer des recomptages parallèles à la liste certifiée des bulletins de vote déchiffrés (1.3.5.b).
- Le système doit permettre à des vérificateurs indépendants de vérifier et de certifier l'intégrité et l'authenticité des composantes du système utilisées pour traiter les urnes (1.3.5.c).

Risque : TRÈS FAIBLE

Comme les résultats du processus de dépouillement seront protégés et que des processus de dépouillement indépendants pourraient être exécutés pour vérifier les résultats obtenus, le niveau de risque résiduel sera très faible.

Menace 4 : Un pirate (externe ou interne) pourrait modifier les résultats d'élection publiés.

Complexité / Probabilité : MOYENNE

Il serait difficile de modifier les résultats de l'élection après le processus de dépouillement et après leur publication, sauf si le site web est hébergé dans un environnement plutôt non sécurisé. Une modification se justifierait par une attaque réussie d'un pirate qui parviendrait à remplacer le contenu du site web. Les attaques internes sont moins réalisables, car le pirate serait repéré sur-le-champ.

Impact : MOYEN

L'image des responsables de l'élection pourrait en prendre pour son rhume.

Atténuation :

- l'information transférée au SGE d'Élections Ontario doit être protégée pour assurer son intégrité et son authenticité (1.3.3.c).
- les modes de diffusion (comme un site web public) doivent être protégés contre les attaques externes.

Risque : TRÈS FAIBLE

Comme les résultats du processus de dépouillement seront protégés et comme l'attaque peut être repérée et résolue facilement, le niveau de risque résiduel sera très faible.

9.1.6 VÉRIFICATION DE L'ÉLECTION

L'inexactitude ou le caractère incomplet des données nécessaires pour étayer une vérification pourrait mettre en péril la vérification de l'élection.

9.1.6.1

VÉRIFIABILITÉ – VÉRIFIABILITÉ INEXACTE

Une traçabilité insuffisante de l'élection ou des données de vérification faciles à altérer peuvent permettre aux pirates de cacher un comportement interdit.

Attaque : les systèmes de vote n'enregistrent pas assez de données de vérification pour vérifier le processus de vote ou de compilation.

Complexité / probabilité : FACILE

Il se pourrait que l'on n'enregistre pas assez (ou pas du tout) de données de vérification pendant le processus de vote.

Impact : ÉLEVÉ

Les résultats de l'élection pourraient être remis en question parce qu'une vérification valide est impossible.

Atténuation :

- Les fichiers journaux du système et les données de l'élection produits au cours de l'élection doivent permettre une vérification significative de l'élection sans exiger que les vérificateurs aient accès à une clé privée ou sans présumer du rôle d'un acteur protégé (2.1.10.b).
- Le système doit permettre aux vérificateurs de retracer tout processus d'élection de façon significative, sans mettre en péril le caractère confidentiel ou exact de l'élection (2.1.10.a).
- Le système doit mettre en œuvre des pratiques cryptographiques adéquates pour vérifier l'exactitude et l'intégrité de l'information des fichiers journaux devant être utilisée pendant la vérification (2.1.10.c).
- Le système doit permettre à tout vérificateur indépendant de vérifier et de certifier l'intégrité des composantes de l'application à tout moment pendant l'élection (2.1.10.d).
- Le fournisseur de service doit décrire son approche d'un processus vérifiable de bout en bout (2.2.5.e).
- Le système doit, à des fins de vérification, permettre de retracer avec exactitude les processus qui ont mené au dépôt et à l'archivage d'un vote dans une urne (2.1.6.c).
- Le système doit faciliter une vérification significative du système par des vérificateurs tiers de confiance sur la base de l'information et des fichiers journaux de l'élection archivés (1.4.2.c).
- Les vérificateurs doivent pouvoir vérifier l'intégrité et l'authenticité de l'information et des fichiers journaux de l'élection pour repérer toute tentative de manipulation de ces données de vérification (1.4.2.e).

Risque : FAIBLE

Comme des mesures de contrôle permettront de s'assurer de l'enregistrement de l'information sur le processus de vote et le processus de compilation, le niveau de risque résiduel sera abaissé à faible.

Menace 1 : Les composantes du système de vote enregistrent des données de vérification contrefaites pour établir qu'une élection frauduleuse était valide.

Complexité / Probabilité : MOYENNE

Il faudrait déployer des efforts pour modifier ou introduire de fausses données de vérification dans les fichiers journaux de l'application.

Impact : ÉLEVÉ

Les résultats de l'élection pourraient être remis en question parce que les données des fichiers journaux sont inexactes ou ont été falsifiées.

Atténuation :

- le système doit mettre en œuvre des pratiques cryptographiques adéquates pour vérifier l'exactitude et l'intégrité de l'information des fichiers journaux devant être utilisée pendant la vérification (2.1.10.c).
- les vérificateurs doivent pouvoir vérifier l'intégrité et l'authenticité de l'information et des fichiers journaux de l'élection pour repérer toute tentative de manipulation de ces données de vérification (1.4.2.e).
- le fournisseur de service doit décrire son approche d'un processus vérifiable de bout en bout (2.2.5.e).

Risque : TRÈS FAIBLE

Comme la vérification externe du processus d'élection passera certes en revue les données de vérification pour s'assurer qu'il n'y a pas eu de gestes frauduleux, le niveau de risque résiduel sera très faible.

Menace 2 : Les données de vérification pourraient être modifiées par un pirate – sans que ce geste soit repéré – pour illustrer qu'une élection frauduleuse était considérée valide, ou pour révoquer une élection valide.

Complexité / Probabilité : MOYENNE

Un pirate devrait posséder des compétences techniques raisonnables pour pouvoir modifier les données de vérification.

Impact : ÉLEVÉ

Les résultats de l'élection pourraient être mis en péril parce qu'ils ne sont pas vérifiables.

Atténuation :

- Le système doit mettre en œuvre des pratiques cryptographiques adéquates pour vérifier l'exactitude et l'intégrité de l'information des fichiers journaux devant être utilisée pendant la vérification (2.1.10.c).
- Les vérificateurs doivent pouvoir vérifier l'intégrité et l'authenticité de l'information et des fichiers journaux de l'élection pour repérer toute tentative de manipulation de ces données de vérification (1.4.2.e).
- Le fournisseur de service doit décrire son approche d'un processus vérifiable de bout en bout (2.2.5.e).

Risque : TRÈS FAIBLE

Comme les données de vérification (fichiers journaux) seront protégées et que le système ne permettra pas que des modifications passent inaperçues, le niveau de risque résiduel sera très faible.

9.2 ÉVALUATION DU RISQUE LIÉ AUX OPÉRATIONS

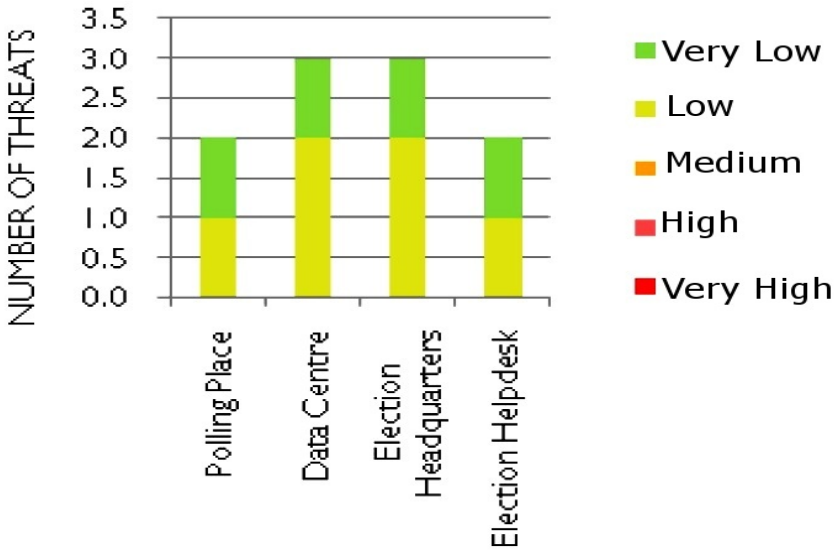
La présente section évalue une série de risques liés aux opérations qui sont associés au modèle de vote en réseau recommandé. Les risques génériques qui s'appliquent à un projet standard ne sont pas évalués. La présente section est structurée en quatre sous-sections, une pour chacun des secteurs opérationnels suivants :

- les bureaux de vote
- le centre de données
- le bureau central d'élections Ontario
- le bureau d'assistance qui soutient l'initiative de vote en réseau.

Le diagramme ci-contre synthétise l'évaluation des risques liés aux opérations touchant le modèle de vote en réseau recommandé dans la présente étude de cas.

Il illustre le nombre de menaces potentielles pour chaque secteur opérationnel, ainsi que le niveau de risque résiduel, compte tenu du fait que des mesures d'atténuation appropriées seraient prises. Comme le montre le diagramme, toutes les menaces opérationnelles qui ont été recensées peuvent être atténuées de manière à limiter le risque résiduel à un niveau faible, voire très faible.

Figure 12 : Risques liés aux opérations



9.2.1 OPÉRATIONS DES BUREAUX DE VOTE

Menace : Les terminaux qui sont utilisés pour voter et/ou pour gérer la liste des votants ne sont pas complètement opérationnels et ne peuvent être utilisés convenablement.

Probabilité : MOYENNE

De nombreux facteurs entrent en jeu dans le processus de mise en place des bureaux de vote, dont le matériel et les logiciels, les communications, les procédures et l'infrastructure. Par conséquent, la probabilité que surviennent des problèmes augmentera en fonction du nombre de bureaux de vote.

Impact : MOYEN

L'indisponibilité de bureaux de vote peut faire en sorte que les votants ne pourront déposer leur vote sans inconvénient, ce qui les contraindra à voter à distance ou à faire de longues queues et pourrait nuire à l'image du SVR.

Atténuation :

- Une équipe de projet chevronnée pourra prévoir les problèmes et planifier en conséquence.
- Des essais adéquats doivent être effectués, dont un test de bout en bout si possible.
- Des mesures de protection adéquates (personnel, équipement, procédures, etc.) doivent être mises en place et mises à l'essai.

Risque : FAIBLE

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau très faible.

Menace : Les responsables de l'élection chargés d'exploiter les diverses composantes du SVR ne peuvent les exploiter correctement.

Probabilité : MOYENNE

Les systèmes devant être exploités ne sont pas très complexes. Cependant, il faut donner de la formation. La probabilité augmente avec le nombre de bureaux de vote.

Impact : FAIBLE

Dans la plupart des cas, ce genre de problème touche un seul membre du personnel de scrutin ou un seul bureau de vote. Il ne devrait donc pas avoir d'effet crucial pour l'ensemble de l'élection.

Atténuation :

- Une formation et du soutien appropriés doivent être donnés aux responsables de l'élection. des équipes de soutien adéquates sont également nécessaires.
- Participation
- Les responsables de l'élection doivent pouvoir utiliser facilement les interfaces du SVR, pour éviter d'être confondus pendant l'exploitation des systèmes et (ou) que leur travail devienne plus difficile et (ou) soit ralenti.
- Les responsables de l'élection qui interagissent avec le SVR doivent être présélectionnés compte tenu de leurs connaissances en informatique.

Risque : TRÈS FAIBLE

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau très faible.

9.2.2 FONCTIONNEMENT DU CENTRE DE DONNÉES

Menace : il manque certaines composantes centrales du SVR qui sont nécessaires, qu'il s'agisse du matériel, du logiciel, ou d'autres produits de communications.

Probabilité : FAIBLE

Il est peu probable que certaines composantes ne soient pas présentes et que ce ne soit pas détecté à temps.

Impact : TRÈS ÉLEVÉ

Des composantes manquantes pourraient avoir un impact majeur sur le rendement du SVR et affecter éventuellement toute l'élection.

Atténuation :

- Une planification adéquate et des essais exhaustifs (dont un plan de rechange) sont nécessaires. des mesures de contrôle périodiques pourraient être mises en place.
- Il faut attribuer suffisamment de temps pour l'acquisition et le déploiement d'un système.
- De solides mesures de sécurité physique doivent être mises en place au centre de données pour empêcher que le personnel non autorisé ait accès au SVR.
- Un système de surveillance faisant rapport des problèmes éventuels devrait être déployé.

Risque : TRÈS FAIBLE

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau très faible.

Menace : Certaines composantes centrales du SVR qui sont nécessaires, qu'il s'agisse du matériel, de logiciels ou de produits de communications connexes, ne fonctionnent pas correctement, par eux-mêmes ou en interaction avec d'autres éléments.

Probabilité : ÉLEVÉE

Les déploiements de centres de données sont très complexes, notamment la configuration de chaque composante et leur intégration comme système unique.

Impact : ÉLEVÉ

La mauvaise configuration ou l'intégration incorrecte d'une composante pourrait avoir un impact majeur sur le rendement du SVR, et, en définitive, affecter l'ensemble de l'élection.

Atténuation :

- Il faut attribuer suffisamment de temps pour le déploiement de système et l'intégration de composantes.
- Il faut effectuer des essais exhaustifs à divers niveaux concernant l'environnement de production réel présent précédemment lors de l'élection.
- Un plan de rechange doit être mis en place.
- Un système de surveillance qui fait rapport des problèmes devrait être mis en œuvre.

Risque : FAIBLE

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau faible.

Menace : les techniciens du centre de données chargés de surveiller le fonctionnement correct de l'infrastructure du SVR se sont comportés de manière incorrecte (intentionnellement ou non).

Probabilité : FAIBLE

Il peut être difficile de mettre en place le centre de données, mais son fonctionnement quotidien ne devrait pas être très complexe.

Impact : TRÈS ÉLEVÉ

Un fonctionnement incorrect ou des procédures incorrectes pourraient affecter l'ensemble de l'élection.

Atténuation :

- Les techniciens du centre de données doivent recevoir une formation appropriée. du personnel de relève doit être disponible.
- Il faut établir des procédures claires qui décrivent comment exploiter le centre de données.
- Des mesures contre la corruption et la contrainte possibles de personnel doivent être prises.
- Un système de surveillance déclarant les défaillances doit être mis en œuvre.
- Le SVR devrait comporter des outils de vérification permettant de vérifier si des actes répréhensibles ont été commis et de déterminer ce qui les a causés.

Risque : FAIBLE

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau faible.

9.2.3 LES OPÉRATIONS DU BUREAU CENTRAL D'ÉO

Menace : les composantes du SVR ne sont ni disponibles ni complètement opérationnelles lorsqu'elles sont nécessaires.

Probabilité : FAIBLE

Le bureau central est un lieu essentiel pour l'élection et est par conséquent très visible. C'est pourquoi il est peu probable que l'une ou l'autre de ses composantes du SVR soit oubliée ou ne soit pas mise à l'essai de manière exhaustive.

Impact : TRÈS ÉLEVÉ

Cette situation pourrait affecter toute l'élection pendant une longue période.

Atténuation :

- Il faut attribuer suffisamment de temps pour l'acquisition et le déploiement d'un système.
- Une planification adéquate et des essais exhaustifs (dont un plan de rechange) sont nécessaires.
- De solides mesures de sécurité physique doivent être mises en place pour le bureau central afin d'empêcher que du personnel non autorisé ait accès au SVR.

Risque : FAIBLE

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau faible.

Menace : Certaines données critiques qui sont nécessaires pour configurer/exploiter le SVR sont incorrectes ou ne sont pas disponibles à temps.

Probabilité : FAIBLE

La façon de fournir des données critiques doit être définie au début du projet, et ce processus ne devrait pas être complexe.

Impact : TRÈS ÉLEVÉ

Certaines données sont des données critiques pour l'élection; sans elles, l'élection ne peut avoir lieu.

Atténuation :

- Définition exacte du format et des procédures des données devant être utilisées par éo.
- Définition exacte des échanges de données.
- Mise à l'essai exacte au moyen de données les plus réelles (contenu, format et volumes) possibles avant l'élection.

Risque : FAIBLE

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau faible.

Menace : Les techniciens chargés d'exploiter les composantes du SVR qui se trouvent au bureau central ne les exploitent pas correctement (intentionnellement ou non).

Probabilité : FAIBLE

Le bureau central est un lieu essentiel pour l'élection et est par conséquent très visible. C'est pourquoi il est peu probable qu'un membre du personnel qui y exploite le SVR ne le fasse pas correctement.

Impact : TRÈS ÉLEVÉ

Cette situation pourrait affecter l'ensemble de l'élection, et y mettre fin pendant une longue période.

Atténuation :

- Les membres du personnel du bureau central doivent recevoir une formation et du soutien adéquats. des équipes de soutien adéquates sont également nécessaires.
- Des procédures claires qui décrivent le mode d'exploitation du SVR doivent être fournies.
- Des mesures contre la corruption et la contrainte possibles de personnel doivent être prises.
- Un système de surveillance déclarant les défaillances doit être mis en œuvre.
- Le SVR devrait comporter des outils de vérification permettant d'établir si des actes répréhensibles ont été commis et de déterminer ce qui les a causés.

Risque : TRÈS FAIBLE

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau très faible.

9.2.4 LES OPÉRATIONS DU BUREAU D'ASSISTANCE

Menace : le bureau d'assistance n'est pas en mesure d'offrir du soutien convenable aux responsables des élections qui utilisent le SVR aux bureaux de vote.

Probabilité : TRÈS FAIBLE

Le nombre de problèmes différents qui peuvent survenir dans les bureaux de vote est limité, et ils devraient pouvoir être réglés facilement. En outre, les membres du personnel du bureau d'assistance seront bien formés et auront accès à des niveaux de soutien additionnels (d'ÉO ou du personnel technique du fournisseur). Il est donc peu probable que le bureau d'assistance ne soit pas en mesure d'offrir le soutien approprié.

Impact : FAIBLE

Atténuation :

- L'équipe de soutien doit compter suffisamment de membres et recevoir une formation adéquate. Il faut également assez de personnel de relève.
- Du soutien de deuxième et de troisième niveau (en quantité suffisante, possédant une formation appropriée et bénéficiant de personnel de relève) doit être disponible.
- Toutes les procédures et tous les guides d'aide (y compris les paliers d'intervention) doivent être élaborés.
- Les outils appropriés du bureau d'assistance doivent être fournis à l'équipe de soutien.

Risque : TRÈS FAIBLE

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau très faible.

Menace : Le bureau d'assistance ne peut fournir un soutien convenable aux votants qui utilisent le SVR à distance.

Probabilité : MOYENNE

Chaque votant peut avoir de nombreux problèmes différents de nature différente, et les membres du personnel du bureau d'assistance éprouveront parfois de la difficulté à les cerner et à les résoudre.

Impact : FAIBLE

Il peut arriver que finalement, quelques votants ne puissent se servir de l'interface de vote à distance; cependant, ils peuvent toujours se rendre dans un bureau de vote.

Atténuation :

- L'équipe de soutien doit compter suffisamment de membres et recevoir une formation adéquate. Il faut également assez de personnel de relève.
- Du soutien de deuxième et de troisième niveau (en quantité suffisante, possédant une formation appropriée et bénéficiant de personnel de relève) doit être disponible.
- Toutes les procédures et tous les guides d'aide (y compris les paliers d'intervention) doivent être élaborés et mis en place.
- Permettre de voter pendant de nombreux jours, afin que les votants à distance qui ne peuvent voter d'un endroit puissent tenter de le faire à partir d'un autre endroit (un autre ordinateur), voire se rendre dans un bureau de vote.

Risque : FAIBLE

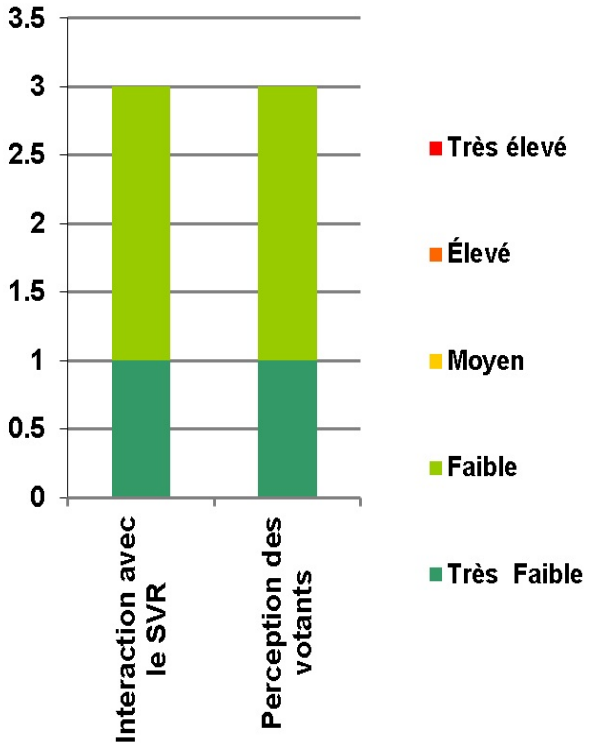
Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau faible.

9.3 ÉVALUATION DU RISQUE LIÉ AU VOTANT

Les risques évalués dans la présente section ont trait aux votants, et incluent leur interaction avec le système de vote en réseau à divers stades, leurs perceptions du système en particulier, et leur perception du vote en réseau en général.

Le diagramme ci-contre synthétise l'évaluation des risques liés au votant qui touchent le modèle de vote en réseau recommandé par la présente étude de cas. Il illustre le nombre de menaces possibles et le niveau de risque résiduel qui serait en place si des mesures d'atténuation appropriées sont prises. Comme l'indique le diagramme, toutes les menaces opérationnelles ayant été établies peuvent être atténuées de manière à limiter le risque résiduel à un niveau faible, voire très faible.

Figure 13 : Évaluation du risque lié au votant



9.3.1 INTERACTION AVEC LE SYSTÈME DE VOTE EN RÉSEAU

Menace : l'interaction avec le SVR n'est ni facile ni intuitive pour les votants.

Probabilité : MOYENNE

La complexité éventuelle du processus d'authentification et (ou) du processus de vote pourrait amener les votants à poser des gestes complexes et à se priver de leur droit de vote.

Impact : MOYEN

La perception qu'a le public d'ÉO et du SVR ne serait peut-être pas aussi bonne qu'on le souhaite.

Atténuation :

- Le système devrait fournir une interface de vote conviviale, afin que le processus de vote soit intuitif et qu'aucune formation préalable ne soit nécessaire pour utiliser le système de vote en réseau (2.3.1.a).
- Le système doit prendre en charge l'utilisation des principaux navigateurs internet et systèmes d'exploitation, et de téléphones courants (2.3.1.b).
- Le système doit inclure des instructions de compréhension facile pour les votants (2.3.1.c).
- Le système doit prévenir les votants si, au cours du processus de vote, ils font une sélection qui pourrait invalider leur vote (p. ex., exercice insuffisant ou excessif du droit de vote. ...) (2.3.1.d).
- Les votants doivent choisir leurs options de vote en sélectionnant directement le candidat plutôt qu'en utilisant un code ou une méthode de sélection indirecte (2.3.1.e).

Risque : FAIBLE

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau faible.

Menace : le système SVR comporte des éléments d'accessibilité insuffisants qui empêchent certains votants de voter par eux-mêmes sans l'aide d'un tiers.

Probabilité : MOYENNE

Le manque d'appareils ou accessoires fonctionnels et (ou) une interface de vote incompatible mineraient la capacité de vote des électeurs ayant certains handicaps.

Impact : MOYEN

Cette situation affectera seulement certains groupes de votants.

Atténuation :

- le système doit prendre en charge l'utilisation de plusieurs langues sans mettre en péril la confidentialité du votant (2.3.2.a).
- le système doit être conforme aux normes d'accessibilité WGAI en matière de suppression de votes (2.3.2.b).
- le système doit soutenir les votants ayant un handicap visuel qui utilisent des lecteurs d'écran (JAWS) et des logiciels de grossissement de texte (2.3.2.c).
- le système doit soutenir les votants ayant un handicap moteur qui utilisent des technologies fonctionnant au souffle ou autres (2.3.2.d).
- les interfaces de vote devraient être validées par des représentants des collectivités de votants ayant un handicap qui utiliseraient lesdites interfaces (votants qui ont un handicap visuel, personnes handicapées, etc.).

Risque : TRÈS FAIBLE

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau très faible.

Menace : le processus d'inscription requis pour utiliser le mode de vote en réseau est trop complexe pour y faire participer une masse critique de votants.

Probabilité : MOYENNE

Le processus d'inscription présenterait une complexité intrinsèque pour certains votants, mais il ne devrait pas affecter la majorité.

Impact : FAIBLE

Advenant une menace, le pourcentage des votants qui utilisent le SVR serait faible, mais la transparence et l'intégrité de l'élection ne seraient pas mises en péril.

Atténuation :

- le processus d'inscription doit être simple et explicite. Si les votants doivent fournir des données personnelles, ils doivent connaître celles-ci facilement.
- les données des votants qui sont archivées dans la base de données doivent être revues pour s'assurer qu'elles ne sont pas trop vieilles ou qu'elles ne renferment pas trop d'erreurs.
- si le processus s'en remet à des tiers (comme le service postal), un processus de rechange doit être mis en place pour tous les problèmes qui s'y rapportent (p. ex. Une livraison au mauvais destinataire, etc.).
- il devrait y avoir d'autres modes d'inscription, voire d'autres modes de scrutin qui ne nécessitent pas un processus d'inscription en particulier (p. ex. voter dans des bureaux de vote en présentant une id régulière).

Risque : TRÈS FAIBLE

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau très faible.

9.3.2 PERCEPTION DU VOTANT

Menace : Les votants peuvent se méfier du SVR et croire qu'il ne respecte pas les principes qui doivent être suivis dans le cadre d'un processus électoral. Cette situation ferait diminuer le nombre de cybervotants.

Probabilité : MOYENNE

Il existe des groupes d'activistes qui sont contre le vote en réseau, mais ils ne forment pas la majorité de la population.

Impact : FAIBLE

La perception du SVR peut être affectée, ce qui fait diminuer le taux de participation. Toutefois, l'impact sur l'élection comme telle ne devrait pas être majeur.

Atténuation :

- un plan de communication exhaustif doit être élaboré afin de s'assurer que tous les votants savent comment le système règle les problèmes éventuels.
- les responsables de l'élection doivent faire preuve de transparence en répondant à toutes les questions qu'ils reçoivent des votants et des autres parties prenantes.
- le SVR devant être utilisé doit pouvoir être expliqué facilement aux citoyens, et toute l'information sur les mesures de sécurité qu'il met en œuvre doit être publique.

Risque : FAIBLE

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau faible.

Menace : Certains votants peuvent tenter de tromper le SVR et croire à tort qu'ils peuvent le faire.

Probabilité : TRÈS FAIBLE

Les personnes qui tenteront de pirater le système et qui saisissent mal le comportement du système sont rares.

Impact : FAIBLE

Advenant une menace, la perception qu'ont les votants du SVR serait affectée, mais seulement dans une faible mesure, car dans un tel cas, quelqu'un d'autre établirait que cette perception était erronée.

Atténuation :

- le SVR doit donner de la rétroaction précise aux votants afin de veiller à ce qu'ils comprennent bien ce qu'ils font (afin qu'ils ne pensent pas qu'ils ont pu voter deux fois ou plusieurs fois, que leur vote n'a pas été déposé, etc.).
- des procédures de vérification du dépôt d'un vote devraient être mises en œuvre.

Risque : très faible

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau très faible.

Menace : La majorité des votants ignorent que des modes de scrutin en réseau sont disponibles.

Probabilité : MOYENNE

Il se peut que l'existence de nouveaux modes de scrutin en réseau ne soit pas bien publicisée et demeure peu connue des gens.

Impact : FAIBLE

Si une majorité des votants ne connaissent pas les modes de scrutin en réseau, le pourcentage des votants qui utilisent le SVR serait faible, mais l'élection comme telle ne serait pas mise en péril.

Atténuation :

- Un plan de diffusion (comportant de la publicité, des campagnes dans les médias, etc.) doit être conçu et exécuté à temps.
- Les parties prenantes principales devraient être consultées activement au cours de l'exécution du projet.
- Diverses parties prenantes et des acteurs importants en Ontario devraient être informés du projet pour pouvoir établir des communications en parallèle.

Risque: très faible

Les mesures d'atténuation proposées abaissent le risque résiduel à un niveau très faible.

10. CRITÈRES DE RÉUSSITE

Le présent chapitre expose une série de critères clés qui joueront un rôle crucial dans la réussite du projet pilote sur le vote en réseau, dont un ensemble de paramètres qui aideront à évaluer les résultats d'un projet pilote sur le vote en réseau.

LA RÉUSSITE DU projet pilote sur le vote en réseau reposera sur les trois séries de critères connexes qui suivent :

1. le projet pilote doit mettre en œuvre un système qui préserve, preuves à l'appui, une **« chaîne de confiance »** ininterrompue contrôlant la détention des données de vote;
2. une équipe de projet chevronnée doit mener à bien une **approche de mise en œuvre** efficace;
3. le projet pilote doit étayer les **principes** de base sur le vote en réseau qui sont définis au chapitre 3, qui précède.

10.1 CHAÎNE DE CONFIANCE

La réussite et l'intégrité d'une élection reposent sur l'absence de toute possibilité d'altération des bulletins de vote pendant ou après le dépôt de ceux-ci. Dans un système de vote en réseau, les données peuvent être altérées si un code malveillant est installé à un point quelconque de la chaîne de détention des bulletins de vote. Pour prouver l'intégrité de l'élection, Élections Ontario doit être en mesure de démontrer que seuls les parties et les logiciels dûment autorisés ont eu accès aux données des bulletins de vote numériques. La vérification doit figurer parmi les priorités. Il faut permettre à des vérificateurs indépendants d'étudier le code source, de vérifier la version et le déploiement du logiciel, d'examiner les fichiers journaux du système pendant le scrutin et enfin d'analyser le processus de dépouillement et les résultats.

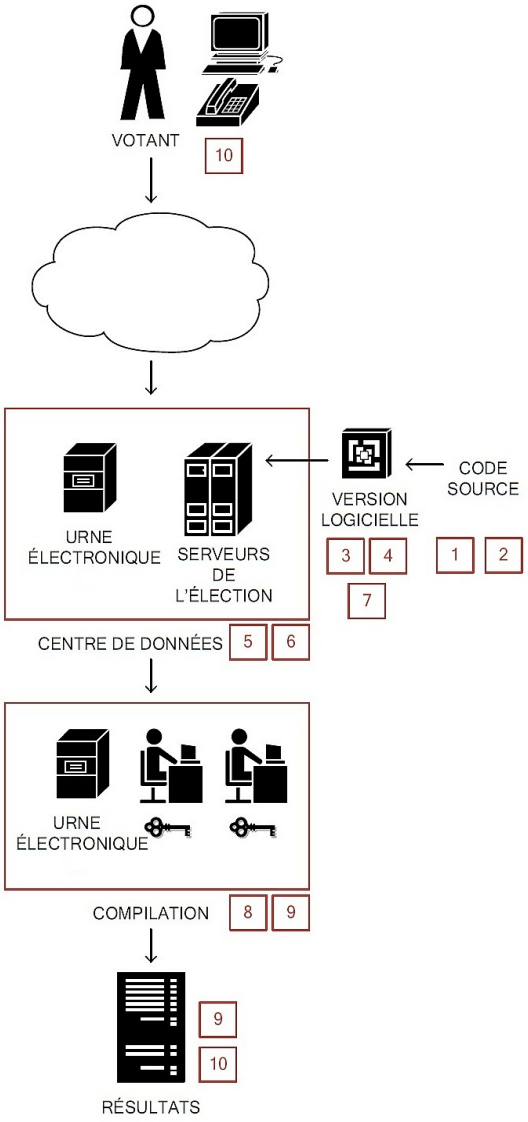
Dans le cas d'une allégation d'altération, la résolution du problème serait fondée sur une investigation informatique : des spécialistes devront valider l'intégrité de la chaîne de confiance en s'appuyant sur la preuve disponible. Si la mise en œuvre du système de vote en réseau ne permet pas à la fois d'établir une chaîne de confiance et de fournir des preuves vérifiables, le processus peut être contesté.

La meilleure façon de prévenir l'existence d'un code malveillant dans un système de vote par internet, présent depuis le début ou ajouté ultérieurement, consiste à avoir recours à des mesures qui en permettent la détection ou la prévention. La chaîne de confiance est le fruit de l'ensemble des mesures suivantes :

1. Vérification du code source permettant de s'assurer que seules les opérations devant être exécutées le seront.
2. Signature numérique du code source vérifié permettant de protéger son authenticité et son intégrité.
3. Création d'une version fiable du code de vote exécutable en présence des vérificateurs (à partir du code source vérifié).
4. Signature du code exécutable permettant de protéger son authenticité et son intégrité.
5. Déploiement du logiciel exécutable sur un système propre.
6. Sceau électronique associé au système afin de détecter tout ajout ultérieurement.
7. Test de cohérence et de précision du système de vote visant à valider son bon fonctionnement.

8. Vérification en continu du système de vote pendant son utilisation au cours de l'élection, par l'examen et la validation des fichiers journaux et d'autres données. Les fichiers journaux doivent être protégés des manipulations externes au moyen de mesures cryptographiques spéciales.
9. Vérification postélectorale validant le comportement du système après examen des sceaux électroniques et des fichiers journaux protégés. Possibilité de recomptages.
10. Vérification individuelle par les votants pour établir que leurs bulletins de vote ont été pris en compte dans le résultat final (grâce à l'envoi d'accusés de réception spéciaux).

Figure 14 : Chaîne de confiance



Si ces processus sont bien appliqués, de concert avec une solution sécurisée de vote en réseau et avec les procédures appropriées, il peut être établi que l'élection s'est bien déroulée et qu'il n'y a pas eu d'altération.

10.2 APPROCHE DE MISE EN ŒUVRE

Élections Ontario doit reconnaître que le projet pilote présentera de multiples sources de risque et doit mettre en œuvre une stratégie pour les gérer. Les risques liés à la mise en œuvre du projet (y compris les risques qui touchent les exigences, la qualité et le calendrier) peuvent être gérés par l'engagement d'une équipe de projet chevronnée, qui doit mener à bien une approche de mise en œuvre efficace s'articulant autour des points suivants :

- acquisition d'un système hôte sécurisé hautement disponible;
- acquisition d'une solution COTS assurant un niveau élevé de sécurité de bout en bout et dont le fournisseur justifie d'une expérience dans le cadre d'élections officielles à grande échelle;
- test approfondi de l'utilisation et des performances;
- démonstrations et examen par les parties prenantes;
- participation dédiée d'experts du domaine chez Élections Ontario visant à assurer l'adaptation sur mesure de la solution;
- consultation suivie visant notamment à élargir le panel des parties prenantes consultées.

Autre facteur de réussite tout aussi important : Élections Ontario devra parvenir à convaincre le public de la sécurité et de l'intégrité du processus par le biais d'une campagne de sensibilisation détaillée démontrant à la fois qu'il existe des préoccupations légitimes et qu'elles sont prises en compte. On misera encore davantage sur les processus qui sont déjà en place à des fins de communications et de sensibilisation.

Fait essentiel, le fournisseur du système de vote en réseau ayant été retenu devrait posséder une expérience confirmée dans des mises en œuvre similaires, notamment de l'expérience de plus d'une élection dans laquelle le client était une administration publique, pour laquelle la liste électorale comprenait au moins 150 000 votants potentiels, et une combinaison de votes à distance et de votes sur site.

Le fournisseur de système devrait également être en mesure de faire la preuve que son produit a réussi des vérifications et (ou) des certifications fiables et mesurables, y compris des vérifications qui prouvent le soutien aux principes clés de l'élection, l'intégrité des données, la force du chiffrement utilisé, de même que la vérifiabilité du code source.

10.3 MESURE DES RÉSULTATS

Pour produire un rapport sur la pertinence de recourir aux technologies de vote en réseau dans la province de l'Ontario, Élections Ontario devra être capable de mesurer les résultats du projet pilote d'après un ensemble concret d'objectifs. Pour établir les meilleurs liens avec les objectifs stratégiques d'élections Ontario, les paramètres recommandés doivent reposer sur la liste de principes de base servant à mesurer le vote en réseau. Voir le chapitre 3 pour prendre connaissance d'un exposé sur le mode de sélection de ces huit principes.

Le tableau qui suit propose des outils d'évaluation et de mesure visant à déterminer le respect de chacun de ces principes. Pendant la mise en œuvre du projet, il est possible de définir des indicateurs de mesure spécifiques et leurs valeurs cibles s'il y a lieu.

PRINCIPE	PARAMÈTRE
Accessibilité[1.2] / facilité d'emploi[1.1]	L'étude de 2007 a révélé que les personnes handicapées étaient confrontées à plus d'obstacles que les autres dans l'exercice de leur droit de vote. La réussite du projet pilote peut être mesurée au moyen d'une étude postélectorale ou d'un sondage des votants pour évaluer les problèmes qui représentent les obstacles : Ajouter aux questions de l'étude de 2007 d'autres questions sur l'expérience du vote en réseau. Comparer avec les données de base de la même circonscription électorale (présumer que des données brutes de la CÉ sont disponibles dans l'étude la plus récente). Recueillir une rétroaction qualitative de la part de groupes d'experts, ce qui établira des paramètres précis établissant que les personnes handicapées étaient plus ou moins satisfaites.
Un votant, un vote[2.1]	Une vérification postérieure à l'événement peut prouver que le vote en réseau n'a pas introduit de risque additionnel : En comparant le nombre d'électeurs qui ont voté avec le nombre de votes déposés; En prouvant qu'il y a seulement 1 vote dans le système pour chaque électeur qui a voté. Il est souhaitable de prouver que c'est véridique non seulement dans le système de vote en réseau, mais également dans l'ensemble des mécanismes. Nécessité de rendre compte des bulletins de vote déposés au moyen des mécanismes en réseau et et des bulletins de vote sur papier déposés sur site. L'exactitude de cette mesure sera fonction de l'établissement d'une liste de votants complète et faisant autorité (en ligne).
Authentification et autorisation du votant[2.4]	L'événement peut être vérifié pour prouver que le processus satisfait au processus en place ou l'améliore. Démontre que le système a fourni un système d'authentification sécurisé. Peut inclure l'examen des mises à jour de la liste des votants. L'exactitude de cette mesure sera fonction de l'établissement d'une liste de votants complète et faisant autorité (en ligne).
Prise en compte des suffrages exprimés par des votants admissibles uniquement[2.6]	L'événement peut être vérifié (antérieurement et postérieurement) pour prouver que le processus satisfait au processus déjà en place ou l'améliore. Relier un bulletin de vote (chiffré) à un votant. Chaque bulletin de vote doit être associé à un votant qui a voté. Le système doit fournir des mécanismes qui appuient les éléments vérifiés (altération, lien « privé » entre votants et bulletins de vote, signatures numériques des bulletins de vote, etc.)
Vérifiabilité au cas par cas[3.2]	En plus des mécanismes visant la facilité d'utilisation qui donnent aux utilisateurs une rétroaction accessible en temps réel, la publication des

PRINCIPE	PARAMÈTRE
	résultats de la vérification après l'élection peut également étayer la vérifiabilité. La réussite de ces mécanismes et d'autres mécanismes peut être mesurée au moyen d'une étude postérieure à l'élection.
Confidentialité[4.3]	Le système peut être vérifié après l'événement pour démontrer que l'identité du votant a été séparée du bulletin de vote lisible du votant.
Validation des résultats[6.4]	Le système peut être vérifié après l'événement pour démontrer que les résultats peuvent être reconstruits de manière indépendante. L'étendue de ces nouveaux calculs peut varier, tout comme l'étendue de la répétition du processus. le traitement des bulletins de vote à cette fin peut constituer des « recomptages » et peut par conséquent nécessiter un pouvoir particulier.
Disponibilité du service[7.1]	La disponibilité du service peut être mesurée techniquement de deux façons : rapports sur la production et la disponibilité, y compris le temps de réponse et des statistiques sur le temps de disponibilité. la disponibilité du service à chaque bureau de vote (connectivité internet, disponibilité des postes de travail et appareils ou accessoires fonctionnels). des ENS seront nécessaires pour tous les paramètres.

11. ESTIMATION DES COÛTS

11.1 ESTIMATION DES COÛTS DU PROJET PILOTE

Le coût estimé d'un projet pilote portant sur les deux modes de scrutin recommandés est établi à 1 745 500,00 $, environ la moitié de cette somme devant être affectée aux coûts de la solution COTS. Ce chiffre correspond au budget total nécessaire pour personnaliser et mettre à l'essai la solution COTS, obtenir une licence pour 100 000 votants à 2 $ par personne, tenir l'élection, procéder au dépouillement et procéder à la vérification de l'intégralité du processus. Il n'inclut pas les coûts des ressources internes.

*deux modes de scrutin à distance

*pas de registre du scrutin

*deux trousses d'inscription

Coûts d'un projet pilote (à distance seulement)	
Solution COTS	$ 837 000,00
Coûts du lieu de vote -	
Infrastructure centrale	$ 162 000,00
Coûts de déploiement	$ 217 500,00
Coûts des ressources du projet	$ 429 000,00
Autres coûts du projet	$ 100 000,00
Total	**$ 1 745 500,00**

Le poste budgétaire COTS inclut le coût de 100 000 permis de votant uniques, ainsi que le coût des services professionnels requis pour adapter et mettre en œuvre une solution de vote en réseau disponible sur le marché. Les coûts du lieu de vote comprendraient le coût du registre du scrutin et du matériel de vote et l'infrastructure de soutien, ce qui représenterait environ 5 000 $ par lieu advenant une mise en œuvre. Comme le vote sur site n'est pas recommandé présentement dans le cadre du projet pilote, et qu'un registre du scrutin électronique n'est pas nécessaire, ce poste demeure à zéro. Le poste infrastructure centrale englobe les coûts de gestion de l'hébergement pour un an, de même que le déchiffrement spécialisé et le matériel de sortie. Les coûts de mise en œuvre comprennent les coûts d'envoi postal de deux trousses d'inscription (156 000 $) et du personnel du bureau d'assistance et de soutien (30 000 $). Le poste des ressources du projet représente le coût de dotation d'une équipe d'exécution spécialisée chargée de la gestion du projet, de l'assurance de la qualité, et de l'intégration aux activités d'élections Ontario. Le dernier poste inclut le coût estimatif des communications et de la sensibilisation.

Cependant, la majorité de ces coûts ne seront pas renouvelés si une seconde élection partielle est organisée la même année. Le poste budgétaire récurrent le plus important correspond à la solution COTS, c'est-à-dire principalement aux coûts de licence des électeurs et d'assistance pendant l'élection. L'autre dépense récurrente correspond au coût associé à la mise en œuvre du scrutin (approbation et déploiement du système, personnel de soutien et envoi de courriers sécurisés). Par conséquent, une deuxième élection partielle comportant 100 000 électeurs et 10 bureaux de scrutin engagerait un total additionnel d'environ 649 500,00 $.

11.2 COÛTS POSSIBLES DE L'ÉLECTION GÉNÉRALE

Bien qu'il s'avère difficile d'estimer avec précision les coûts inhérents à une élection générale, il est important de noter qu'un facteur clé est susceptible de changer : les frais de licence facturés par un fournisseur de solution COTS ne s'élèveront plus qu'à 0,25 $ par utilisateur. Si le vote par ordinateur était mis en œuvre jusqu'au nombre maximal de lieux (environ 600), le coût total d'une élection générale serait de 9 295 500,00 $.

Coûts d'une élection générale	Initiaux	Récurrents	Total
Solution COTS	$ 478,500.00	$ 2,331,500.00	$ 2,810,000.00
Coûts du lieu de vote	$ 2,910,000.00	$ 261,000.00	$ 3,171,000.00
Infrastructure centrale	$ 162,000.00	$ -	$ 162,000.00
Coûts de déploiement	$ 12,000.00	$ 2,611,500.00	$ 2,623,500.00
Coûts des ressources du projet	$ 429,000.00	$ -	$ 429,000.00
Autres coûts du projet	$ 50,000.00	$ 50,000.00	$ 100,000.00
Total	**$ 4,041,500.00**	**$ 5,254,000.00**	**$ 9,295,500.00**

Il est à noter qu'en raison d'un coût de licence par votant beaucoup plus bas, les coûts sont répartis plus également entre les postes COTS, lieu de vote, et mise en œuvre. Les coûts de mise en œuvre récurrents sont élevés, surtout en raison du besoin récurrent de courrier sécurisé et de personnel de soutien.

MISE EN GARDE

Les facteurs de coût principaux doivent être étudiés plus avant : le besoin de réinvestir dans les ressources de projet peut évoluer suivant les résultats du projet pilote, et les besoins liés à l'infrastructure centrale peuvent augmenter pour soutenir le trafic additionnel des votants. Il existe une variable majeure concernant les coûts des fournisseurs. Les coûts qui font l'objet de cette étude sont fondés sur un examen des prix de l'industrie et peuvent évoluer considérablement dans le contexte d'une soumission concurrentielle ou d'une négociation de contrat.

Estimation détaillée par poste

	Quantité	Unité	Coût unitaire	Total
1. Coût de la solution COTS (adaptation et intégration)				**$ 837 000,00**
Système VR	**28**	**750**	**1000**	**$ 783 000,00**
Licence du logiciel	**100000**		**2**	**$ 200 000,00**
Services connexes				**$ 583 000,00**
Adaptation de logiciel (dont le système d'inscription en ligne)	6	GCH	$ 16 500,00	$ 99 000,00
Intégration aux systèmes d'ÉO (SGE, inscription de votant, RVI)	2	GCH	$ 16 500,00	$ 33 000,00
Déploiement au centre de données, dont le renforcement du SE	3	GCH	$ 16 500,00	$ 49 500,00
Mises à l'essai (à divers niveaux)	2	GCH	$ 16 500,00	$ 33 000,00
Soutien EAU	2	GCH	$ 16 500,00	$ 33 000,00
Soutien durant le processus électoral, dont la configuration	2,5	GCH	$ 16 500,00	$ 41 250,00
Soutien au processus de vérification	1	GCH	$ 22 000,00	$ 22 000,00
Soutien postélectoral	0,5	GCH	$ 16 500,00	$ 8 250,00
Conseils spécialisés en cybervote	3	GCH	$ 22 000,00	$ 66 000,00
Mise en œuvre de la gestion du projet	6	GCH	$ 22 000,00	$ 132 000,00
Gestion du projet - élection	3	GCH	$ 22 000,00	$ 66 000,00
Vérificateur tiers	3	GCH	$ 18 000,00	**$ 54 000,00**
2. Matériel du bureau de scrutin				**$ -**
	par endroit	*totaux*	*coût unitaire*	
Meubles				
Pupitres/tables (réutilisation de biens existants)				$ -
Cloisonettes (réutilisation de biens existants)				$ -
Téléphones de vote (dont le matériel faisant double emploi)				**$ -**
Téléphones	0	0	$ 20,00	$ -
Casques d'écoute pour téléphones	0	0	$ 20,00	$ -
Bouchons jetables pour casques d'écoute	0	0	$ 0,25	$ -
Ordinateurs de vote (+matériel faisant double emploi)	0			**$ -**
Ordinateurs à écran tactile	0	0	$ 850,00	$ -
Appareils fonctionnant à souffle	0	0	$ 750,00	$ -
Molettes/manettes	0	0	$ 250,00	$ -
Clavier et souris	0	0	$ 50,00	$ -
Logiciel de lecture d'écran	0	0	$ 800,00	$ -
Casques d'écoute pour ordinateurs	0	0	$ 25,00	$ -
Bouchons jetables pour casques d'écoute	0	0	$ 0,25	$ -
Carte à puce intelligente	0	0	$ 25,00	$ -
Imprimante (pour accusés de réception)	0	0	$ 150,00	$ -
Registre du scrutin	0			**$ -**
Ordinateur/écran	0	0	$ 600,00	$ -
Imprimante	0	0	$ 150,00	$ -
Lecteur de carte à puce	0	0	$ 25,00	$ -
Cartes à puce	0	0	$ 20,00	$ -
Coûts d'emplacement (infrastructure)	0			**$ -**
Lignes téléphoniques	0	0	$ 130,00	$ -
Connexions du réseau aux bureaux de scrutin (double emploi)	0	0	$ 135,00	$ -
Connexions du réseau aux bureaux de scrutin (double emploi)2	0	0	$ 300,00	$ -
Courant de relève	0	0	$ 500,00	$ -
Interrupteurs, routeurs	0	0	$ 150,00	$ -
Câbles	0	0	$ 5,00	$ -
3. Infrastructure centrale				**$ 162 000,00**
Infrastructure du centre d'appels				$ 30 000,00
Coûts du centre de données (service géré pendant 1 an, inclut disponibilité élevée)				$ 125 000,00
Infrastructure de déchiffrement et de dépouillement				$ 7 000,00

4. Coûts de déploiement				**$ 217 500,00**
Déploiement du système				**$ 22 000,00**
Certification du matériel (téléphones, ordinateurs de votes, ordinateurs du RSé)	0	GCH	$ 22 000,00	$ -
Examen de candidat / approbation de bulletins de vote	0,25	GCH	$ 22 000,00	$ 5 500,00
Exemple de système (pour examen de candidat et partie prenante)	0,75	GCH	$ 22 000,00	$ 16 500,00
Déploiement et déclassement	0	GCH	$ 22 000,00	$ -
Trousse d'inscription (devant inclure l'identificateur unique de VR du votant)				**$ 156 000,00**
Enveloppes d'envois postaux sécurisés	100000		0,15	$ 15 000,00
Impression				$ 8 000,00
Frais postaux	-		0,59	$ 55 000,00
2e envoi postal (taux en pourcentage reflétant la mise en œuvre)	100%			$ 78 000,00
Personnel de soutien				**$ 30 000,00**
Centre d'appels (1ère ligne)	2	GCH	$ 10 000,00	$ 20 000,00
Bureau d'assistance (2e ligne)	1	GCH	$ 10 000,00	$ 10 000,00
Équipes techniques	0	GCH	$ 10 000,00	$ -
Membres du personnel de scrutin				**$ -**
Secrétaire du bureau de vote (augmentation nette de 1 à 2 semaines x 10 emplacements)	0	GCH	$ 5 000,00	$ -
Formation				**$ 9 500,00**
Membres du personnel de scrutin	0	GCH	$ 10 000,00	$ -
Équipes de soutien	0	GCH	$ 10 000,00	$ -
Centre d'appels	0,25	GCH	$ 10 000,00	$ 2 500,00
Bureau d'assistance	0,25	GCH	$ 10 000,00	$ 2 500,00
Personnel du bureau du directeur de scrutin	0,1	GCH	$ 10 000,00	$ 1 000,00
Personnel du bureau des révisions	0,1	GCH	$ 10 000,00	$ 1 000,00
Formation du personnel d'ÉO (bureau central)	0,25	GCH	$ 10 000,00	$ 2 500,00
5. Coûts des ressources du projet (projet de 4,5 mois)				**$ 429 000,00**
Lancement du projet (1 PM)	3	GCH	$ 22 000,00	$ 66 000,00
Gestion et planification de projet (1 PM) pendant le déploiement	4,5	GCH	$ 22 000,00	$ 99 000,00
Gestion et planification de projet (1 PM) pour l'élection	0	GCH	$ 22 000,00	$ -
Conception et développement (BA, SA,)	5	GCH	$ 22 000,00	$ 110 000,00
Architecture technique (valider la sécurité et la conception de l'infrastructure)	3	GCH	$ 22 000,00	$ 66 000,00
Intégration à la liste des votants - SGE (analyste-programmeur)	2	GCH	$ 22 000,00	$ 44 000,00
Essai du système (1 gestionnaire)	0	GCH	$ 22 000,00	$ -
EAU/test de groupe de réflexion (AAC)	2	jours	$ 22 000,00	$ 44 000,00
6. Autres coûts du projet				**$ 100 000,00**
Déplacements : visites de site, conférences				$ 50 000,00
Sensibilisation				**$ 50 000,00**
Télé, publicités imprimées (pas d'augmentation nette)				
Consultation des parties prenantes (phase II) Études et recherche sur le vote en réseau				$ 50 000,00
Courriel de sensibilisation (pas d'augmentation nette)				
TOTAL GÉNÉRAL				**$ 1 745 500,00**

12. CONCLUSIONS ET RECOMMANDATIONS

LA PRÉSENTE ÉTUDE DE CAS a examiné et évalué la liste des quatre scénarios de vote en réseau retenus :

1. le vote sur site par ordinateur,
2. le vote sur site par téléphone,
3. le vote à distance par ordinateur,
4. le vote à distance par téléphone.

Les quatre scénarios peuvent bien fonctionner dans le cadre de la plupart des contraintes documentées qui sont mises en place pour un projet pilote. Toutefois, les modes de scrutin sur site instaureront davantage de complexité opérationnelle et de changements organisationnels qu'Élections Ontario pourrait être prêt à accepter pour le déploiement à court terme d'un projet pilote. Comme l'investissement dans le changement requis pour faire face à la complexité accrue ne procurerait que l'avantage négligeable de fournir des options de vote en réseau à seulement un sous-groupe d'électeurs qui, autrement, ne seraient pas en mesure d'avoir accès au vote par téléphone ou par internet, Élections Ontario pourrait envisager d'éliminer les modes de scrutin sur site du projet pilote.

12.1 OPTIONS DE MISE EN ŒUVRE

L'évaluation a également porté sur des options de mise en œuvre dans deux domaines clés : l'authentification du votant et la gestion de la liste des votants.

Options d'authentification du votant

D'après l'évaluation, le recours à un document d'identification émis par le gouvernement pour confirmer les déclarations d'identité des électeurs s'avère la méthode la plus sécurisée. Cependant, Élections Ontario a uniquement accès aux données des permis de conduire et, dans ce cas, les électeurs non détenteurs d'un permis de conduire ne peuvent pas s'inscrire par le processus ordinaire. Élections Ontario peut alors décider de privilégier l'accessibilité plutôt que la sécurité. Un processus d'inscription reposant sur une forme moins sécurisée de renseignements à caractère personnel (adresse et date de naissance), mais qui introduit un avantage marginal en matière de sécurité grâce à l'envoi d'un second courrier, permettrait à tous les électeurs de l'Ontario d'accéder au même processus. Élections Ontario doit également accepter le fait que cette option, certes plus accessible, rallonge les délais du processus et rend ainsi le vote en réseau plus complexe — ce qui peut s'accompagner d'une baisse de l'utilisation générale et réduire par la même occasion la taille de l'échantillon sur lequel se fondera le rapport présenté à l'Assemblée législative en 2013.

Options de gestion de la liste des votants

Si Élections Ontario élimine les modes de scrutin sur site pour les motifs exposés précédemment, un registre du scrutin en ligne en temps réel ne sera pas nécessaire à proprement parler. Élections Ontario peut plutôt mettre en œuvre des mesures de contrôle du processus afin de prévenir la possibilité de votes multiples au moyen de plusieurs modes de scrutin. Ces mesures de contrôle comprendraient essentiellement une date-limite d'inscription qui accorde du temps pour imprimer et distribuer les registres du scrutin sur papier avant le début de la période de vote par anticipation. Ces registres du scrutin indiqueraient quels votants se sont inscrits pour voter en ligne, afin que les membres du personnel de scrutin puissent les empêcher de déposer des bulletins de vote en personne, ce qui soutiendrait le principe « un votant, un vote ».

12.2 CONCLUSIONS

Les quatre scénarios de mode de scrutin retenus pourraient fonctionner dans le cadre des limites d'Élections Ontario et présenteraient des avantages à une multitude d'électeurs ontariens. Cependant, certains facteurs clés peuvent influer sur l'équation coûts-avantages. Plus précisément, les avantages du vote en réseau sur site, qui ne procurent qu'un avantage marginal du point de vue de la commodité et de l'accessibilité du votant, ne valent peut-être pas l'investissement requis dans le cadre d'un projet pilote. même si ces modes de scrutin peuvent faire l'objet d'un projet pilote comportant des dépenses en immobilisations relativement peu élevées, notamment s'il est question d'un seul lieu, le coût pour Élections Ontario est élevé sur le plan de la complexité et du besoin en changement organisationnel.

Cette complexité engloberait les changements de personnel (nouvelles compétences des membres du personnel de scrutin), de processus (gestion de la liste électronique des électeurs en temps réel), et de systèmes (nouvelles interfaces avec les systèmes existants de gestion des élections). Compte tenu du fait que cette étude de cas recommande les options viables seulement dans le contexte d'un projet pilote, l'ampleur du changement ne vaut peut-être pas l'investissement. L'objectif principal du projet pilote, qui consiste à mesurer la faisabilité du vote en réseau pour faire rapport en toute confiance sur une orientation future pour l'Ontario, peut être atteint sans consacrer de l'argent à la mise en œuvre du vote sur site.

Une fois que la portée du projet pilote a été déterminée, Élections Ontario doit également décider s'il va quand même mettre en œuvre un registre du scrutin électronique et comment configurer le processus d'inscription : pour la sécurité ou pour l'accessibilité.

12.3 RECOMMANDATIONS

1. Le déploiement de modes de scrutin à distance uniquement peut permettre d'atteindre les objectifs du projet pilote. Au vu de la complexité et du coût de déploiement des modes de scrutin en réseau sur site et des bénéfices marginaux offerts en termes d'accessibilité, investir dans cette solution pour le projet pilote ne se justifie pas.
2. L'authentification des votants est l'un des huit principes fondamentaux que doit étayer le projet pilote. Pourtant, le processus associé est à l'origine de plusieurs risques majeurs en matière de sécurité, notamment du risque d'usurpation d'identité des votants. L'atténuation de ces risques repose en partie sur l'intégration de renseignements à caractère personnel dans le processus d'inscription des votants, dans le but de confirmer leurs déclarations d'identité. à l'heure actuelle, l'option la plus sécurisée consiste à recourir à un document d'identification émis par le gouvernement, à savoir le numéro de permis de conduire.

ACCÈS NON UNIVERSEL À L'AUTHENTIFICATION PAR NUMÉRO DE PERMIS DE CONDUIRE

Bien que la vérification de l'identité des utilisateurs par ce biais constitue la meilleure solution à ce jour, ce moyen pénalise directement les votants se trouvant dans l'incapacité d'obtenir un permis de conduire. Ce compromis peut sembler acceptable dans le cadre du projet pilote, mais Élections Ontario devra tout de même utiliser une forme d'identification plus universelle ou d'autres renseignements à caractère personnel lors des prochaines échéances électorales.

ÉLABORER UN MODÈLE D'AUTHENTIFICATION PLUS UNIVERSEL

Les possibilités de mise en œuvre d'une méthode d'authentification plus universelle existent et doivent être approfondies. Élections Ontario doit mener simultanément ses recherches dans deux directions :

- l'utilisation d'un renseignement à caractère personnel plus universel que le numéro de permis de conduire pour vérifier l'identité des électeurs lors de leur inscription;
- L'intégration et l'exploitation d'un mécanisme d'authentification tiers, comme le projet ServiceOntario.

Aux fins du projet pilote, Élections Ontario peut envisager d'instaurer un mode d'inscription moins robuste, mais plus accessible, par exemple, le processus d'envoi par la poste en trois étapes décrit au chapitre 6.

LE PROJET PILOTE DE VOTE À DISTANCE N'IMPLIQUE PAS LA CRÉATION D'UN REGISTRE DU SCRUTIN ÉLECTRONIQUE

3. Si le vote en réseau était proposé à la fois à distance et sur site, les menaces créées par la mise à la disposition en parallèle de plusieurs modes de scrutin (papier, ordinateur et téléphone) et de différents types d'authentification (physique et mot de passe) mettraient en péril deux principes fondamentaux : la capacité à garantir qu'un seul vote par votant est pris en compte et la nécessité de compter uniquement les suffrages exprimés par des votants admissibles. Pour atténuer ces menaces, il faudrait prévoir un registre du scrutin en ligne mis à jour en temps réel qui gérerait simultanément le vote en réseau et le mode de scrutin sur papier. En l'absence de registre du scrutin électronique, les votants pourraient voter deux fois : une fois en ligne et une fois en personne.

Toutefois, en éliminant le vote en réseau sur site, le risque qu'un votant vote plusieurs fois est réduit et il s'avère plus difficile de justifier la création d'un registre du scrutin électronique, au vu des facteurs de coût et de complexité. Dans ce scénario, le risque peut être contrôlé en autorisant les votants inscrits pour le vote en réseau à voter uniquement à distance. Leurs noms n'apparaissant pas sur les registres du scrutin physiques, ces votants ne peuvent pas déposer un bulletin de vote sur papier pendant la période de vote par anticipation

LE VOTE PAR TÉLÉPHONE PRÉSENTE DES RISQUES, MAIS ACCROÎT L'ACCESSIBILITÉ DU VOTE

4. Le vote par téléphone présente des risques intrinsèques parmi les plus difficiles à gérer ou à atténuer convenablement. Ces risques découlent du fait que le vote par téléphone utilise une infrastructure impossible à sécuriser de la même façon qu'un réseau informatique. Les lignes téléphoniques publiques ne sont pas sécurisées, ce qui crée des risques sur le plan de la confidentialité. Ensuite, les suffrages ne sont pas chiffrés au sein de l'environnement RVI, où ils peuvent donc être interceptés, lus, voire modifiés. Cependant, l'inclusion du vote par téléphone améliore considérablement l'accessibilité du vote en réseau au sein des segments de la population qui n'ont pas accès à un ordinateur et à internet ou qui ne sont pas à l'aise avec ces technologies. Ces risques peuvent être atténués dans une certaine mesure, principalement grâce à la sécurisation de l'environnement RVI et au déploiement de systèmes de détection des intrusions. La suppression du vote par téléphone affaiblirait la conformité aux principes du projet, mais permettrait aussi de réduire les risques, les coûts et la complexité.

ÉLECTIONS ONTARIO DOIT CONTRÔLER L'ENVIRONNEMENT HÔTE

5. La capacité d'Élections Ontario à contrôler du mieux possible l'environnement de vote en réseau sera un élément capital dans l'instauration et le maintien de la chaîne de confiance. Par conséquent, Élections Ontario doit faire l'acquisition d'un environnement hôte (Web + RVI notamment) en vertu d'un accord distinct du contrat d'achat de la solution COTS, et le fournisseur sélectionné devra préciser en détail ses besoins sur le plan du matériel et de l'infrastructure. sinon, la demande de propositions (DP) doit stipuler que le serveur hôte est physiquement dédié au projet électoral, afin que les serveurs puissent être scellés en vertu du principe de la chaîne de confiance aux fins d'assurer sa vérifiabilité.

L'approche recommandée pour la mise en œuvre du vote en réseau consiste par conséquent à proposer un mode de scrutin par téléphone et un mode de scrutin par internet lors d'une prochaine élection partielle. La réalisation d'un projet pilote en vertu du modèle général décrit au chapitre 6, mais sans mode de scrutin sur place, permettra de procéder dans le respect des contraintes opérationnelles d'élections Ontario, des principes électoraux fondamentaux, de l'orientation stratégique et des objectifs définis.

APPENDICE A : EXIGENCES DÉTAILLÉES

1. EXIGENCES FONCTIONNELLES

1.1 EXIGENCES PRÉALABLES À L'ÉLECTION

1.1.1 GESTION DE L'INFORMATION AVANT L'ÉLECTION

Exigences ayant trait à l'accès à l'information portant sur le système électoral existant (p. ex., les interfaces de saisie d'information, le soutien à la SGLE /au SGE, les types d'élections pris en charge, les méthodes de dépouillement pris en charge, etc.)

a. Le système doit être en mesure d'automatiser l'importation de l'information sur l'élection tirée des systèmes d'élections Ontario. Cette information peut notamment porter sur :

- la date et l'heure du début et de la fin de la période de vote
- les circonscriptions électorales
- les bulletins de vote (noms des candidats).

b. Le système doit protéger l'intégrité et l'authenticité de l'information sur l'élection qui est utilisée pour configurer la plateforme de vote.

1.1.2 INSCRIPTION DANS LA LISTE ÉLECTORALE ET GESTION DES JUSTIFICATIFS D'IDENTITÉ

Exigences ayant trait à la gestion de l'information sur le votant et des justificatifs d'identité (p. ex., création de l'ID d'électeur pour chaque électeur, distribution des justificatifs d'identité, gestion de l'inscription, etc.).

a. Le système doit être en mesure d'automatiser l'importation d'informations externes de la liste électorale en provenance du SGE / SGLE.

b. Le système doit être en mesure de produire une id d'électeur unique pour chaque votant admissible.

c. Le système doit être en mesure d'exporter des données afin de fournir à la carte d'avis d'enregistrement (sous l'impulsion du système SGE/SGLE) assez de données pour charger et distribuer les id d'électeur par courrier.

d. Le système doit fournir une interface web permettant aux votants de s'inscrire au vote en réseau.

I. Les votants doivent être en mesure d'entrer l'ID d'électeur reçu dans la carte d'avis d'enregistrement dans un site web sécurisé (dont l'adresse est fournie sur la carte d'avis d'enregistrement)

II. Les votants doivent être en mesure d'entrer dans le site web des données personnelles supplémentaires pour aider Élections Ontario à vérifier leur identité. Il pourrait s'agir de leur date de naissance et d'une pièce d'identité émise par le gouvernement.

III. Après l'authentification, et au cours de la même séance, le site web doit fournir aux votants un mot de passe numérique unique et fort ou permettre au votant de choisir son propre mot de passe, pourvu qu'il respecte les normes de sécurité exigées.

e. Le système doit fournir une interface de réponse vocale interactive (RVI) qui permet aux votants de s'inscrire en vue du vote en réseau.

I. Les votants doivent être en mesure d'entrer l'ID d'électeur reçue sur la carte d'avis d'enregistrement en composant le numéro sans frais imprimé sur cette carte et en utilisant une interface de RVI.

II. Les votants doivent être en mesure d'entrer dans l'interface de RVI des données personnelles supplémentaires pour aider Élections Ontario à vérifier leur identité. Il pourrait s'agir de leur date de naissance et d'une pièce d'identité émise par le gouvernement.

III. Après l'authentification, et au cours de la même séance, le système RVI doit fournir aux votants un mot de passe numérique unique et fort ou permettre au votant de choisir son propre mot de passe, pourvu qu'il respecte les normes de sécurité exigées.

f. Le système doit être en mesure d'interagir avec le SGE d'ÉO pour prendre en charge les éléments en ligne en temps réel du registre du scrutin.

1.1.3 CONSEIL CENTRAL DE GESTION DU VOTE EN RÉSEAU

Exigences liées à l'existence d'un conseil de gestion du vote en réseau qui doit certifier l'information sur l'élection.

a. Le système doit permettre la configuration sécurisée du conseil de gestion du vote en réseau de façon à ce qu'un nombre minimal de membres soit requis pour procéder au déchiffrement, pour compiler et pour établir le résultat final des votes, dans le but d'empêcher qu'un membre seul agisse par lui-même.

b. Le système doit exiger la présence du conseil de gestion du vote en réseau pour certifier tout changement à la configuration de l'élection.

c. Le conseil de gestion du vote en réseau doit certifier toute information sur l'élection au moyen de pratiques de non-répudiation (p. ex., des signatures numériques).

   I. L'information sur l'élection comprend : la liste des votants[18], la liste des candidats/bulletins de vote, et les données concernant les heures d'ouverture, etc.

   II. L'information sur l'élection devrait porter une signature numérique afin que tout vérificateur puisse valider le fait que le système de vote configuré reflète les données fournies par ÉO.

d. Les processus précédents doivent être exécutés dans un serveur isolé ne comportant pas d'accès à un réseau pour assurer une protection sécuritaire maximale.

1.1.4 VÉRIFICATION PRÉALABLE À L'ÉLECTION

L'information sur l'élection qui est utilisée par la plateforme de vote au cours du processus de vote et de dépouillement doit être vérifiable afin qu'il soit possible de repérer toute tentative de manipulation. L'information sur l'élection est perçue comme toute autre information en format électronique qui est utilisée par la plateforme de vote ou par des vérificateurs indépendants pour vérifier la configuration correcte de l'élection. Cette vérification comprend le contenu de la liste électorale, les modèles de bulletin de vote, l'identification aux fins de l'élection, les membres du conseil de gestion du vote en réseau, et ainsi de suite.

a. Le système doit vérifier si l'information sur l'élection a été certifiée électroniquement par le conseil de gestion du vote en réseau avant de lancer les processus de vote et de dépouillement.

b. Le système doit permettre à tout vérificateur indépendant de vérifier si l'information sur l'élection qui a été utilisée par la plateforme de vote a été certifiée par le conseil de gestion du vote en réseau.

En outre, les diverses composantes de logiciel de la plateforme de vote doivent également être certifiées pour détecter toute tentative d'altération. Ainsi, il devrait être plus facile pour les vérificateurs indépendants et les votants de vérifier si les composantes utilisées sont les mêmes que celles qui ont été vérifiées.

c. Les vérificateurs indépendants doivent être en mesure de vérifier et de certifier les composantes utilisées pour voter. Cette vérification devrait comprendre minimalement :

I. la révision des mesures de sécurité mises en œuvre dans le logiciel (p. ex., des protocoles et algorithmes cryptographiques);

II. la révision du code source, dont la mise en œuvre des mesures de sécurité mentionnées précédemment;

III. un test fonctionnel;

IV. un test d'exactitude.

d. Les votants doivent être en mesure de vérifier l'intégrité et l'authenticité de toute composante de vote exécutée sur l'appareil de vote avant de s'en servir (p. ex., vérification de la signature numérique d'un applet java lors de l'utilisation d'un ordinateur pour voter).

e. Tout vérificateur indépendant doit être en mesure de certifier l'intégrité et l'authenticité des composantes du système qui sont installées dans la plateforme de vote.

f. Toute action exécutée par un vérificateur indépendant ne doit avoir d'incidence ni sur la confidentialité ni sur l'intégrité de l'élection.

1.1.5 PRODUCTION DES JUSTIFICATIFS D'IDENTITÉ DU VOTANT

a. La plateforme de vote doit interagir avec le SGE d'Élections Ontario pour obtenir la liste des votants qui recevront une carte de la poste.

b. La plateforme de vote doit fournir les justificatifs d'identité du votant exigés au SGE (le code d'utilisateur), afin qu'ils puissent être imprimés sur les cartes qui doivent être envoyées à tous les votants.

c. La plateforme de vote doit protéger tous les mots de passe connexes de manière à ce que seuls les membres du personnel autorisés d'Élections Ontario puissent y avoir accès. Les administrateurs de système ne peuvent avoir accès aux mots de passe.

1.1.6 INSCRIPTION À DISTANCE

a. La plateforme de vote doit fournir une interface web aux votants pour qu'ils puissent obtenir leur mot de passe en ligne, une fois qu'ils ont saisi le système de l'ID qu'ils ont reçu par la poste et d'autres renseignements personnels.

b. Une interface similaire doit être mise à la disposition des votants qui utilisent le téléphone (interface sonore qui fonctionne avec la RVI fournie par élections Ontario).

1.2 EXIGENCES LIÉES AU PROCESSUS DE VOTE

1.2.1 ACCÈS À LA PLATEFORME DE VOTE

Exigences liées à l'accès à la plateforme de vote (p. ex., ordinateurs des votants pris en charge, installation gratuite, etc.)

Dans le cas du vote à distance par ordinateur :

a. La plateforme de vote doit permettre aux votants de déposer leurs bulletins de vote à partir d'ordinateurs qui exploitent des systèmes d'exploitation et des navigateurs couramment utilisés.

b. Les votants ne doivent pas être tenus d'installer manuellement des logiciels ou du matériel d'élection précis dans leurs ordinateurs pour avoir accès au processus de vote, sauf s'ils sont nécessaires à des fins de sécurité et (ou) d'accessibilité.

c. Les votants ne doivent pas être tenus d'utiliser toujours le même ordinateur de vote (ou adresse IP) pour avoir accès à la plateforme de vote. En d'autres termes, ils pourraient s'inscrire à un endroit et voter dans un autre endroit.

d. Les votants doivent être en mesure de vérifier l'authenticité de la plateforme de vote à laquelle ils accèdent au moyen de leur navigateur.

Dans le cas du vote sur site :

e. Les votants doivent pouvoir s'identifier eux-mêmes auprès d'un membre du personnel de scrutin en utilisant une identification acceptée par la loi. Le système doit offrir une interface au membre du personnel de scrutin afin qu'il valide l'admissibilité du votant (p. ex. Les votants figurent sur la liste des votants et n'ont jamais voté auparavant).

f. Le système doit fournir un genre de jeton (p. ex. Carte à puce intelligente ou NIP sur un morceau de papier) au votant, afin qu'il puisse voter à l'aide de l'un des terminaux de votation disponible (ordinateurs ou téléphones) dans le bureau de vote.

Dans le cas du vote sur site par ordinateur :

g. La plateforme de vote doit permettre aux votants de déposer leurs bulletins de vote à l'aide d'appareils informatisés accessibles et conviviaux qui se trouvent dans le bureau de vote, dont les technologies d'aide au vote suivantes :

    I. logiciel de lecteur d'écran

    II. appareils de saisie fonctionnant au souffle

    III. manettes

    IV. écrans tactiles.

Dans le cas du vote par téléphone :

h. La plateforme de vote doit permettre aux votants de déposer leurs bulletins de vote à l'aide d'appareils téléphoniques réguliers, analogiques ou numériques, qu'il s'agisse de téléphones conventionnels, de téléphones qui fonctionnent à base de voix sur IP (VOIP) et de téléphones mobiles.

1.2.2 AUTHENTIFICATION DES VOTANTS

Exigences liées à l'authentification des votants.

Authentification à distance :

a. Le système doit exiger que les votants se servent de justificatifs d'identité en particulier pour accéder au système de vote.

b. Les justificatifs d'identité du votant doivent être combinés aux données personnelles pour donner accès au système de vote afin de déposer un bulletin de vote.

c. Les votants doivent être en mesure d'avoir accès au système de vote à plusieurs reprises de divers endroits et appareils pourvu qu'ils ne déposent pas de bulletin de vote.

Authentification sur site :

d. Les votants doivent être en mesure de s'identifier devant un membre du personnel de scrutin au moyen d'une ID acceptée par la loi. Si le votant est admissible à voter, il obtiendra un jeton pour avoir accès au système de vote.

e. Le système de vote (sur site) doit accepter le jeton et valider son authenticité pour donner accès au votant.

1.2.3 FORMAT DU BULLETIN DE VOTE (OPTIONS DE VOTE)

a. L'option de vote doit se présenter en format clair et compréhensible, sans être codifiée ni nécessiter le recours à une table de codage révélant la valeur véritable des options.

b. Les votants doivent être en mesure de distinguer clairement les diverses options de vote (candidats).

c. Les options de vote doivent pouvoir prendre en charge l'utilisation de langues multiples, présentement indiquées dans le système comme anglais et français.

d. Le bulletin de vote doit être organisé de manière à pouvoir présenter les noms de candidats en ordre fixe (alphabétique) ou aléatoire.

1.2.4 SÉLECTION ET CONFIRMATION DES OPTIONS DE VOTE

L'écran du bulletin de vote en ligne ou le menu RVI doit être assez facilement utilisable pour que les votants puissent distinguer clairement leurs choix et être mis en garde contre des choix faits par mégarde ou d'autres erreurs. Toutefois, la fonction de l'option de vote devrait permettre l'exercice insuffisant du droit de vote.

a. Le système devrait prévenir et avertir les votants dans l'éventualité où ils commettent des erreurs involontaires qui pourraient invalider leur vote (p. ex., il devrait empêcher l'exercice excessif du vote et mettre en garde contre l'exercice insuffisant involontaire du vote).

b. Le système devrait distinguer clairement les options de vote sélectionnées des options non sélectionnées.

c. Le système doit permettre aux votants de déposer des bulletins de vote vierges.

d. Le système doit permettre aux votants de vérifier leurs options de vote avant de déposer leur bulletin de vote.

e. Le système doit donner au votant l'option de modifier son vote avant de le déposer.

f. Le système doit donner au votant l'option de refuser intentionnellement le bulletin de vote. Le bulletin de vote refusé devrait être inscrit dans le système.

g. Le système RVI doit donner au votant l'option d'augmenter ou de diminuer la vitesse et le volume de lecture, et de répéter les options du menu.

h. Le système RVI doit confirmer clairement les sélections de bulletin de vote et permettre aux votants d'annuler l'opération et de procéder à une nouvelle saisie au besoin.

1.2.5 DÉPÔT DU BULLETIN DE VOTE

a. Le système doit indiquer clairement au votant à quel moment le bulletin de vote est déposé et s'il a été archivé correctement ou non dans le système de vote.

b. Lans le cas du vote par ordinateur, le système doit protéger la confidentialité et l'intégrité du vote déposé de même que l'identité du votant par des moyens cryptographiques, de manière à ce que le vote ne puisse être altéré pendant son transport ou son archivage.

c. Lans le cas du vote par ordinateur, le système doit également permettre aux votants de protéger leurs votes dans leur ordinateur de vote avant de le déposer, plutôt que seulement lorsque les serveurs de l'élection reçoivent les votes.

d. Les votes déposés doivent être protégés contre les attaques externes et internes (p. ex. par les administrateurs de système) en ayant recours à des mesures cryptographiques adéquates pouvant être démontrées devant un expert en matière de sécurité ou un vérificateur.

e. Lorsque c'est possible, utiliser le chiffrement dans les voies de communications.

f. En ce qui concerne le vote par téléphone, le système doit mettre en œuvre des procédures appropriées pour atténuer les attaques internes ou externes qui pourraient avoir une incidence sur la confidentialité du votant et (ou) l'intégrité des bulletins de vote.

1.2.6 VÉRIFIABILITÉ DU VOTANT

Le système doit permettre aux votants en réseau de vérifier qu'Élections Ontario a reçu leurs votes à la fin de l'élection, et qu'ils ont par conséquent été inclus dans le dépouillement final.

a. Le système doit fournir aux votants un accusé de réception une fois qu'ils ont déposé leur vote. Cet accusé de réception leur permettra de vérifier que leur vote était présent pendant le processus de déchiffrement et de dépouillement

b. L'accusé de réception de vote doit comprendre une preuve d'authenticité pour éviter les fausses déclarations faites par des votants (p. ex. Une signature numérique).

c. Sur demande, le système doit permettre aux votants de prouver que leur vote était présent lors du dépouillement final.

d. Toute méthode de vérification des votants ne doit pas faciliter la contrainte ou l'achat de votes en incluant des preuves lisibles de la sélection effective du votant.

e. L'accusé de réception de vote ne doit pas permettre de lier les votants aux bulletins de vote qu'ils ont déposés ou aux accusés de réception. Ainsi, leur confidentialité est assurée.

1.2.7 LA GESTION DES VOTANTS PENDANT LE PROCESSUS DE VOTE

Le système de vote en réseau doit prendre en charge les exigences suivantes liées à la gestion des votants pendant le processus de vote.

a. Le système doit permettre aux utilisateurs autorisés d'invalider des votants avant et pendant le processus de vote (p. ex. Si le mécanisme d'authentification du votant a été mis en péril et s'il doit être bloqué). Si un votant ayant déjà déposé un vote a fait l'objet d'une invalidation, le vote doit être indiqué comme invalide et ne pas être utilisé dans le dépouillement final.

b. Le système doit permettre aux utilisateurs autorisés de poser les gestes suivants :

    I. ajouter de nouveaux votants à l'élection si la loi l'exige;

II. produire de nouveaux justificatifs d'identité pour le vote en réseau;

III. émettre de nouveau les justificatifs d'identité perdus;

IV. supprimer un votant et annuler ses justificatifs d'identité;

V. mettre à jour le dossier d'un votant si sa circonscription électorale a changé.

c. L'une ou l'autre des actions précédentes ne doit pas affecter la confidentialité du votant ou l'intégrité de l'élection.

1.2.8 SURVEILLANCE DE L'ÉLECTION

Il devrait être possible de démontrer aux parties prenantes et aux vérificateurs, entre autres, que le système de vote en réseau n'a pas fait l'objet d'une intrusion ou d'une manipulation de données. Pour ce faire, il convient de disposer d'outils de surveillance.

a. Le système de vote doit fournir des outils de surveillance qui détectent les anomalies au cours du processus de vote.

b. Le système doit s'assurer que les outils de surveillance sont protégés contre les altérations et offrent la non-répudiation de l'information de vérification enregistrée.

c. Le système de vote doit garantir que les outils de surveillance ne peuvent mettre en péril la confidentialité du votant et l'exactitude de l'élection.

1.3 DÉPOUILLEMENT ET PUBLICATION DES RÉSULTATS

1.3.1 CLÔTURE DU PROCESSUS DE VOTE

Il doit être possible de lancer clairement et sans ambiguïté la clôture de la période de vote.

a. Le système doit clore automatiquement l'élection au moment indiqué par Élections Ontario pendant l'organisation de l'élection et ne doit pas permettre que cette date et cette heure soient dépassées.

b. Les votants ne doivent pas être autorisés à avoir accès au système et à déposer leurs votes après la clôture du processus de vote.

c. Le système doit donner aux votants qui sont en train de déposer leur vote plus de temps pour achever de le faire.

d. Le système doit empêcher les pirates internes ou externes (dont les acteurs possédant des droits d'accès privilégié au système) d'ajouter des votes des votants qui n'ont pas participé, une fois que l'élection est close.

e. Le système doit protéger l'intégrité et l'authenticité de l'urne électronique (qui renferme tous les votes déposés par les votants) une fois que le processus de vote est clos (p. ex., en signant numériquement l'urne).

1.3.2 DÉCHIFFREMENT ET COMPILATION DES URNES ÉLECTRONIQUES

Une fois que la période de vote a pris fin, les résultats du vote en réseau (notamment le vote par ordinateur et par téléphone) doivent être déchiffrés et dépouillés.

a. Le processus de déchiffrement et de dépouillement doit être exécuté dans un environnement isolé qui n'est branché à aucun réseau.

b. Le transfert de l'urne ou des urnes électronique(s) des serveurs de l'élection à l'environnement isolé doit assurer l'intégrité et l'authenticité de l'urne.

c. L'authenticité et l'intégrité des urnes recueillies doivent être vérifiées avant que celles-ci soient acceptées.

d. Les urnes doivent renfermer tous les votes déposés pendant le processus de l'élection (i.e., si le vote multiple est requis, tous les votes déposés par les votants doivent être inclus dans l'urne recueillie).

e. Le processus de déchiffrement et d'établissement du résultat ne peut être lancé que par une majorité préalablement définie de membres du conseil de gestion du vote en réseau, qui doivent se réunir pour reconstruire la clé de déchiffrement.

f. Le processus de déchiffrement et d'établissement du résultat doit vérifier que tous les votes contenus dans les urnes ont été déposés par des personnes ayant les qualités requises pour voter.

g. Le processus de déchiffrement et d'établissement du résultat doit empêcher le déchiffrement de votes multiples du même votant, notamment en empêchant de dépouiller les votes qualifiés d'invalides par un utilisateur autorisé (comme dans les cas de déclaration d'usurpation d'identité).

h. Le processus de déchiffrement et d'établissement du résultat doit veiller à ce qu'il soit impossible d'établir une corrélation entre l'ordre des bulletins de vote déchiffrés et l'ordre de leur dépôt et, par conséquent, empêcher tout lien entre les bulletins de vote déchiffrés et les votants (p. ex., en ayant recours à un processus de mélange).

i. Le conseil de gestion du vote en réseau doit certifier la liste des bulletins de vote déchiffrés (p. ex., en les signant numériquement).

j. Le processus de déchiffrement et d'établissement du résultat doit garantir qu'il est impossible d'établir une corrélation entre les données de vérification du votant (p. ex., les accusés de réception de vote) et les options de vote choisies sur le bulletin de vote.

1.3.3 CONSOLIDATION DES RÉSULTATS DE L'ÉLECTION

a. Les bulletins de vote déchiffrés qui ont été obtenus du processus précédent doivent être transférés au système de gestion de l'élection (SGE) d'Élections Ontario en vue d'une consolidation avec les résultats obtenus des autres modes de scrutin (par la poste et sur papier, sur site).

b. L'information transférée au SGE d'Élections Ontario doit être protégée pour assurer son intégrité et son authenticité.

c. Élections Ontario conviendra du contenu détaillé des données qui doivent être transférées ainsi que de leur format pour atténuer les changements apportés à son SGE.

1.3.4 CERTIFIER ET PUBLIER LES RÉSULTATS ÉLECTRONIQUES

a. Le système doit produire les résultats du mode de vote en réseau à partir de la liste certifiée des bulletins de vote déchiffrés.

b. Le système doit publier les résultats du vote en réseau avec l'information qui permet au votant de vérifier son vote. Le système doit inclure une interface simple qui permet à Élections Ontario de recueillir de l'information et de l'afficher dans son site web (p. ex. Un service web).

c. Le système doit être en mesure de produire des rapports de résultats, y compris ce qui suit :

- tous les bulletins de vote acceptés/valides pour chaque candidat par CÉ/CP;
- tous les bulletins de vote refusés;
- tous les bulletins de vote non marqués;
- tous les bulletins de vote invalides;
- le nombre total de votes par cas (accepté, refusé, non marqué, et invalide) par mode (par téléphone, par ordinateur) et par endroit (sur site, à distance).

d. Pour chaque circonscription électorale, le système doit exporter et distribuer au coordonnateur des résultats de la circonscription électorale un rapport de résultats qui inclut le dépouillement de votes.

1.3.5 VÉRIFICATION DU PROCESSUS DE DÉPOUILLEMENT

a. Le système doit permettre à des vérificateurs indépendants ou au conseil de gestion du vote en réseau d'exécuter de nouveaux processus de déchiffrement et de compilation au besoin.

b. Le système doit permettre aux vérificateurs indépendants de procéder à un nouveau décompte, en parallèle de la liste certifiée des bulletins de vote déchiffrés. Les vérificateurs doivent être en mesure de travailler à partir des bulletins de vote déchiffrés et d'obtenir des résultats traduits en clair susceptibles d'être comparés à ceux qui sont générés par le système.

c. Le système doit permettre aux vérificateurs indépendants de vérifier et de certifier l'intégrité et l'authenticité des composantes du système utilisées pour traiter les urnes électroniques, y compris l'authenticité des logiciels, l'intégrité du système, l'intégrité et l'authenticité des fichiers journaux générés, etc.

1.4 VÉRIFICATION DES RÉSULTATS

1.4.1 VÉRIFICATION DES RÉSULTATS PAR LE VOTANT

a. Le système doit générer un accusé de réception de vote qui permet aux votants de vérifier que leur vote s'est rendu au conseil de gestion du vote en réseau et était présent au cours du processus de déchiffrement et d'établissement du résultat.

b. Cet accusé de réception doit permettre aux votants de remplir une déclaration valide s'ils se rendent compte que leur vote n'a pas été traité.

c. Le système doit fournir aux votants une interface leur permettant de vérifier facilement leurs accusés de réception. Cette interface devrait être disponible dans le site web d'élections Ontario.

1.4.2 VÉRIFICATION INDÉPENDANTE DE L'ÉLECTION

a. Les vérificateurs doivent avoir accès au code source du système si Élections Ontario le demande.

b. Le fournisseur doit fournir les procédures, les technologies et le mécanisme requis pour assurer un processus de vérification de bout en bout, de la construction du système de vote en réseau à la validation des résultats de l'élection.

c. Le système doit faciliter une vérification significative du système par des vérificateurs tiers de confiance sur la base de l'information et des fichiers journaux de l'élection archivés.

d. Le système doit permettre d'effectuer une vérification complète sans mettre en péril l'intégrité de l'élection et la confidentialité du votant.

e. Les vérificateurs doivent pouvoir vérifier l'intégrité et l'authenticité de l'information et des fichiers journaux de l'élection pour repérer toute tentative de manipulation de ces données de vérification.

2. PRINCIPES ET EXIGENCES NON FONCTIONNELLES

2.1 PRINCIPES UNIVERSELS

2.1.1 FACILITÉ D'UTILISATION

Le processus de vote doit être facile à comprendre et à exécuter par les votants. Les votants ne doivent pas avoir besoin de compétences techniques, culturelles ou législatives particulières pour exprimer un suffrage.

a. Le système devrait fournir une interface de vote conviviale, afin que le processus de vote soit intuitif et qu'aucune formation préalable ne soit nécessaire pour utiliser le système de vote en réseau.

b. Le système doit prendre en charge l'utilisation des principaux navigateurs internet et systèmes d'exploitation, et de téléphones courants.

c. Le système doit comprendre des instructions de compréhension facile pour les votants.

d. Le système doit prévenir les votants si, au cours du processus de vote, ils font une sélection qui pourrait invalider leur vote (p. ex., exercice insuffisant ou excessif du droit de vote, etc.)

e. Les votants doivent choisir leurs options de vote en sélectionnant directement le candidat plutôt qu'en utilisant un code ou une méthode de sélection indirecte.

2.1.2 ACCESSIBILITÉ

Le processus de vote doit être également accessible à tous les votants admissibles, y compris les votants handicapés. Quoi qu'il en soit, le votant doit exécuter le processus de vote sans avoir besoin d'aide pour effectuer ses sélections.

a. Le système doit prendre en charge l'utilisation de plusieurs langues sans mettre en péril la confidentialité du votant.

b. Le système doit être conforme aux normes d'accessibilité WGAI en matière de suppression de votes et aux directives pour l'accessibilité aux contenus web de niveau AA (DACW 2.0).

c. Le système doit soutenir les votants ayant un handicap visuel qui utilisent des lecteurs d'écran (JAWS, NVDA, VoiceOver, etc.) et des logiciels de grossissement de texte.

d. Le système doit soutenir les votants ayant un handicap moteur qui doivent utiliser un bulletin de vote sonore (au moyen du téléphone ou d'un lecteur d'écran), et des appareils fonctionnant au souffle et autres appareils de saisie de type molette/manette.

e. L'interface de RVI doit permettre aux votants d'ajuster les facteurs suivants :

    I. La vitesse du contenu et la capacité d'ajuster la vitesse de lecture

    II. La capacité d'ajuster le niveau du volume de lecture

    III. La capacité de répéter ou de rebobiner les menus et d'autres contenus, ainsi que les sélections de l'utilisateur

    IV. La durée du délai d'inactivité imposé dans les sélections de l'utilisateur

2.1.3 FACILITÉ D'ATTEINTE (EMPLACEMENT)

Tout votant doit avoir accès facilement aux méthodes de vote, indépendamment de l'emplacement physique du votant pendant la période de vote.

2.1.4 UN VOTE PAR VOTANT

Un seul vote par votant est dénombré pour obtenir les résultats de l'élection. Cette règle doit être suivie même si le votant a le droit de déposer des votes multiples.

2.1.5 PAS DE VOTANTS PRIVILÉGIÉS

Aucun votant (individuel ou groupe) ne doit posséder un avantage technique, logique ou décisionnel sur les autres votants. Chaque vote a la même valeur, peu importe le votant qui le dépose.

2.1.6 AUCUN ACTEUR PRIVILÉGIÉ

Aucune personne ni entité impliquée dans la gestion ou l'application du processus électoral ne doit pouvoir influer sur ce processus ni recueillir de l'information qui n'est pas publique.

2.1.7 AUTHENTIFICATION ET AUTORISATION DU VOTANT

Le processus électoral doit s'assurer, avant de permettre à un votant de déposer un vote, que l'identité du votant est bien l'identité prétendue, que l'électeur est admissible à voter, et que les intentions de vote permises n'ont pas été excédées.

Dans le cas de l'authentification à distance :

a. Les justificatifs d'identité du votant doivent être combinés aux données personnelles pour donner accès au système de vote afin de déposer un bulletin de vote.
b. Le système doit exiger que les votants se servent de justificatifs d'identité en particulier pour accéder au système de vote.
c. Les votants doivent être en mesure d'avoir accès au système de vote à plusieurs reprises de divers endroits et appareils pourvu qu'ils ne déposent pas de bulletin de vote.

Dans le cas de l'authentification sur site :

d. Les votants doivent être en mesure de s'identifier devant un membre du personnel de scrutin au moyen d'une id acceptée par la loi. Si le votant est admissible à voter, il obtiendra un jeton pour avoir accès au système de vote.
e. Le système de vote (sur site) doit accepter le jeton et valider son authenticité pour donner accès au votant.

2.1.8 DROIT DE FIGURER SUR LA LISTE DES VOTANTS

Le processus électoral doit s'assurer que tous les votants admissibles sont inclus dans la liste des votants et que tous les votants peuvent faire valoir leur droit de vote s'ils n'y figurent pas.

2.1.9 PRISE EN COMPTE DES SUFFRAGES EXPRIMÉS PAR DES VOTANTS ADMISSIBLES UNIQUEMENT

Le processus électoral doit veiller à ce que les votes dépouillés dans le cadre du processus de dépouillement ont été déposés par des votants admissibles à voter.

a. Le système doit garantir que seuls les votants admissibles peuvent entrer dans la plateforme de vote.

b. Avant d'accepter un vote déposé, le système doit vérifier l'identité du votant qui dépose le vote.

c. Le système doit empêcher un votant de déposer plus de votes que le nombre autorisé.

d. Le système doit permettre de vérifier à tout moment pendant l'élection que les votes déposés dans l'urne sont bien ceux de votants admissibles.

e. Le système doit garantir la non-répudiation des votes déposés.

f. Le système doit empêcher l'ajout de bulletins de vote contrefaits dans l'urne par des utilisateurs externes et des administrateurs du système.

g. Le système doit avoir recours à des certificats numériques uniques pour authentifier les votants.

h. Le système doit utiliser des certificats numériques uniques du votant pour signer numériquement les votes déposés.

2.1.10 ORGANISATION JUSTE DU BULLETIN DE VOTE

Le processus de vote doit veiller à ce que toutes les options de vote, les parties et les candidats possèdent le même droit de figurer sur le bulletin de vote. La conception du bulletin de vote ou la distribution des options de vote ne doit favoriser aucun parti ni candidat. Ce principe devrait être préservé indépendamment du mode de scrutin utilisé par le votant pour déposer le vote.

a. L'option de vote doit se présenter en format clair et compréhensible, sans être codifiée ni nécessiter le recours à une table de codage révélant la valeur véritable des options.

b. Les votants doivent être en mesure de distinguer clairement les diverses options de vote (candidats).

c. Les options de vote doivent pouvoir prendre en charge l'utilisation de langues multiples, présentement indiquées dans le système comme anglais et français.

d. L'organisation du bulletin de vote doit pouvoir présenter les noms de candidats en ordre fixe (alphabétique) ou aléatoire.

2.1.11 ABSENCE DE COÛT POUR LES VOTANTS

Les votants ne doivent pas engager de coûts précis dans l'exercice de leur droit de vote. ni le mode de scrutin par ordinateur ni le mode de scrutin par téléphone ne devrait amener le votant à engager des frais directement liés à l'exercice du droit de vote.

2.1.12 PRODUCTION D'UNE LISTE DE VOTANTS JUSTE

Le processus électoral doit utiliser une liste des votants produite honnêtement qui se fonde uniquement sur des données de votants admissibles. Tous les votants admissibles doivent être inclus dans la liste des votants.

2.1.13 NI CONTRAINTE NI VENTE DE VOTES

Le processus de vote doit empêcher la contrainte et la vente de vote, généralement en ne fournissant pas au votant ou à un autre tiers de l'information qui pourrait être utilisée par la personne qui contraint ou par l'acheteur de votes pour deviner comment le votant entend voter.

a. Le système doit produire des accusés de réception de vote qui ne permettent pas aux votants de prouver à un tiers pour qui ils ont voté.

b. Le système doit empêcher quiconque, même les gestionnaires et les vérificateurs protégés, d'établir une corrélation entre les votes et les votants.

2.1.14 VÉRIFIABILITÉ AU CAS PAR CAS

Le processus de vote doit donner aux votants des moyens de vérifier que leurs votes ont été bien déposés dans l'urne (vote enregistré tel que déposé).

a. Le système doit permettre aux votants de vérifier si leurs votes étaient présents pendant le processus de déchiffrement et d'établissement du résultat, au moyen d'un accusé de réception de vote.

b. L'accusé de réception du vote doit protéger le secret du vote (c.-à-d. que l'on ne devrait jamais pouvoir déduire les options de vote retenues).

c. Le processus de vérification doit permettre de détecter les accusés de réception manipulés ou contrefaits pour empêcher les déclarations frauduleuses des votants.

2.1.15 INTÉGRITÉ

Le processus de vote doit veiller à ce que l'issue de l'élection représente l'opinion des votants participants et qu'elle soit par conséquent obtenue seulement à partir des votes déposés par des votants admissibles. De plus, le processus de vote doit veiller à ce que les votes des votants admissibles n'ont pas été manipulés ou à ce qu'il n'y ait pas eu de remplissage d'urne.

a. Le système doit protéger l'intégrité de chaque vote déposé pendant tout le processus électoral.

b. Le système doit permettre de vérifier l'intégrité de chaque vote déposé dans l'urne.

c. L'intégrité du vote est protégée par le votant lorsqu'il dépose son vote au moyen d'un ordinateur.

d. Le système doit empêcher toute tentative d'ajouter des bulletins de vote contrefaits dans l'urne électronique.

e. L'intégrité du vote devrait être protégée au moyen d'un chiffrement fort, comme les signatures numériques.

2.1.16 CONFIDENTIALITÉ DES DONNÉES PERSONNELLES

L'information liée aux votants doit être utilisée seulement aux fins spécifiques de l'élection et aucun acteur non autorisé ne peut y avoir accès. Les votants doivent être protégés contre le vol d'identité.

2.1.17 SECRET DU BULLETIN DE VOTE

Le processus de vote doit préserver le secret des bulletins de vote déposés jusqu'à ce qu'ils doivent être traités dans le cadre du processus de dépouillement.

a. Le système doit garantir qu'un bulletin de vote déposé demeure secret devant les tiers, dont les administrateurs de système et les pirates éventuels qui franchissent les mesures de sécurité traditionnelles qui protègent la plateforme de vote.

b. Les votes doivent être chiffrés dans le terminal du votant avant le dépôt lorsque le votant vote par ordinateur.

c. Les votes peuvent être déchiffrés seulement par le Conseil de gestion du vote en réseau.

d. Le système doit empêcher le déchiffrement des bulletins de vote avant la clôture de l'élection pour éviter toute fuite d'information sur les résultats partiels.

e. Tout processus de vérification pris en charge par le système pour vérifier l'exactitude de l'élection ne doit pas mettre en péril la confidentialité.

2.1.18 CONFIDENTIALITÉ

Le processus de vote doit empêcher à tous les stades de l'élection que l'on puisse établir une corrélation entre les votants et le contenu des bulletins de vote déposés par ces votants.

a. Le système doit garantir que les votes sont chiffrés d'une façon que seul le Conseil de gestion du vote en réseau peut déchiffrer.

b. Le système doit garantir que la clé nécessaire pour déchiffrer les votes n'est pas disponible pendant le processus de vote jusqu'à ce que le Conseil de gestion du vote en réseau la retire/la reconstitue.

c. Le système doit garantir qu'au moins une majorité établie au préalable des membres du Conseil de gestion du vote en réseau est nécessaire pour retirer la clé de déchiffrement de l'élection.

d. Le système doit garantir qu'il est impossible d'établir une corrélation entre l'ordre dans lequel les votes ont été déchiffrés et l'ordre dans lequel ils ont été déposés.

e. Le système doit garantir que deux votes différents dont le contenu est identique présentent des formats de chiffrement différents.

f. Tout processus de vérification pris en charge par le système pour vérifier l'exactitude de l'élection ne doit pas mettre la confidentialité en péril.

2.1.19 PAS DE RÉSULTATS INTERMÉDIAIRES

Le processus de vote doit empêcher tout accès au contenu des votes déposés jusqu'au processus de dépouillement.

a. Le système doit garantir que seul le Conseil de gestion du vote en réseau peut déchiffrer les votes, après une élection, idéalement dans un environnement isolé.

b. Le système doit chiffrer les votes dans le terminal du votant avant de les envoyer au serveur de l'élection.

2.1.20 DÉCLASSEMENT DES DONNÉES PROTÉGÉES

Le processus de vote doit comporter des pratiques de déclassement sécurisées du matériel, des dossiers et des données de vote qui pourraient mettre en péril la confidentialité des votants. Les données électorales, y compris les données saisies et archivées par le système de vote en réseau, doivent être archivées de manière sécuritaire et déclassées après une période définie.

2.2 PRINCIPES PROCÉDURAUX

2.2.1 FORMATION DU VOTANT

Le processus électoral devrait procurer des moyens d'apprendre et de comprendre le processus de vote avant l'élection. Une campagne de communication détaillée sensibilisera et soutiendra efficacement la communauté des électeurs.

2.2.2 INFORMATION/DIFFUSION

Le public devrait avoir accès à de l'information liée au processus électoral (calendrier, technologie, procédures, résultats de vérification, etc.). L'information doit être exacte et disponible assez longtemps avant l'élection. Une campagne de communication détaillée sensibilisera et soutiendra efficacement la communauté des électeurs.

2.2.3 FACILITÉ À EXPLIQUER / COMPRENDRE PAR LES VOTANTS

Le processus électoral doit être aussi simple et facile à comprendre que possible. Une campagne de communication détaillée sensibilisera et soutiendra efficacement la communauté des électeurs.

2.2.4 VÉRIFIABILITÉ DU CODE SOURCE

Le code source et les codes binaires de tout logiciel utilisé pour gérer les processus ou les données de l'élection doivent être disponibles à des fins de vérification et, au besoin, de certification. Le processus de vérification doit être mené à bien par des vérificateurs indépendants afin que le processus électoral se déroule bien.

2.2.5 VÉRIFIABILITÉ DU PROCESSUS

Les procédures suivies pendant le processus de l'élection doivent être bien documentées et vérifiables afin que l'on puisse s'assurer qu'elles sont conformes aux exigences prévues.

a. Le système doit permettre aux vérificateurs de retracer tout processus d'élection de façon significative, sans mettre en péril le caractère confidentiel ou exact de l'élection.

b. Les fichiers journaux du système et les données de l'élection produits au cours de l'élection doivent permettre une vérification significative de l'élection sans exiger que les vérificateurs aient accès à une clé privée ou sans présumer du rôle d'un acteur protégé.

c. Le système doit mettre en œuvre des pratiques cryptographiques adéquates de vérification de l'exactitude et de l'intégrité des renseignements provenant de fichiers journaux qui doivent être utilisés pendant la vérification.

d. Le système doit permettre à tout vérificateur indépendant de vérifier et de certifier l'intégrité des composantes de l'application à tout moment pendant l'élection.

e. Le fournisseur de service doit décrire son approche d'un processus vérifiable de bout en bout.

2.2.6 CERTIFICATION

Le processus de vote et toute logique des composantes physiques qui y sont liées doivent être conçus pour faciliter la certification des éléments principaux de leur conception. La certification confirmera que le processus électoral de vote en réseau peut accomplir ce qui est établi dans les spécifications.

2.2.7 VALIDATION DES RÉSULTATS

Le processus de vote doit offrir une façon de vérifier si les résultats représentent clairement l'intention des votants qui ont participé au processus de vote. Cette vérification doit également assurer que seuls les votes des votants admissibles ont été utilisés dans le processus de dépouillement pour empêcher les pratiques frauduleuses qui pourraient mettre en péril l'exactitude de l'élection.

2.2.8 SURVEILLANCE DE L'ÉLECTION

Le processus de l'élection doit soutenir la surveillance de l'élection pour toutes les transactions effectuées au cours du processus. Ce processus de surveillance doit être solide et garantir que le secret du votant est préservé en tout temps.

2.2.9 EXAMEN DE FICHIERS JOURNAUX/INVESTIGATION INFORMATIQUE

Le processus de l'élection doit laisser des traces des activités exercées au cours du processus (p. ex. des fichiers journaux). Ces traces doivent être disponibles pour analyse pendant et après l'élection afin que l'on puisse s'assurer que le processus électoral se déroule bien.

2.2.10 REPRISES PARTIELLES POSSIBLES

Le processus de l'élection doit permettre la reprise d'une élection active à partir du même stade auquel elle a été stoppée sans perte de l'information qui était déjà enregistrée.

2.2.11 DISPONIBILITÉ DU SERVICE

Le processus de l'élection et toutes ses composantes ou entités essentielles (p. ex., information sur la liste électorale, votes déposés, mode de scrutin, etc.) doivent être à la disposition des votants, des gestionnaires de l'élection, des observateurs ou de tout autre acteur impliqué dans le processus pendant toute la période électorale.

2.2.12 PAS DE POINT DE CONFIANCE UNIQUE

Le processus de l'élection ne doit accorder sa confiance à aucune entité unique (personne ou système) pour la mise en œuvre d'une étape essentielle. Les privilèges de l'entité doivent être limités par les politiques sur la répartition des tâches, afin d'exiger la collaboration de plusieurs entités de mise en œuvre des processus essentiels.

2.2.13 INTÉGRITÉ DE LA PLATEFORME

Le processus de l'élection doit fournir des moyens de protéger l'intégrité et l'authenticité des entités et des composantes qui prennent part au processus. Ces moyens doivent être vérifiables au cours du processus de l'élection, afin que l'on puisse s'assurer de leur fonctionnement correct. Les procédures de vérification peuvent être exécutées avant et après le processus de l'élection.

2.2.14 CONTRÔLE D'ACCÈS

Le processus de l'élection doit fournir des moyens de contrôler et d'enregistrer l'accès des entités aux différentes étapes et composantes utilisées dans le cadre du processus.

2.2.15 INTÉGRITÉ DE L'URNE

Le processus de l'élection doit fournir des moyens de préserver et de détecter toute manipulation de l'urne.

a. Le système doit permettre de vérifier l'intégrité et l'identité du service qui a géré l'urne, avant de lancer le processus de déchiffrement et d'établissement des résultats.

b. Le système doit empêcher l'ajout de votes contrefaits par des utilisateurs externes et des administrateurs du système.

c. Le système doit, à des fins de vérification, permettre de retracer avec exactitude les processus qui ont mené au dépôt et à l'archivage d'un vote dans une urne.

d. Le système doit mettre en œuvre des mesures adéquates pour détecter les anomalies au cours du processus de vote.

2.2.16 INTÉGRITÉ DES FICHIERS JOURNAUX

Le processus de l'élection doit fournir des moyens de préserver et de détecter toute manipulation des fichiers journaux ou registre des activités enregistrées pendant le processus.

2.2.17 INTÉGRITÉ DE LA LISTE DES VOTANTS

Le processus de l'élection doit fournir des moyens de préserver et de détecter toute manipulation des données de la liste électorale.

2.2.18 INTÉGRITÉ DE LA CONFIGURATION DE L'ÉLECTION

Le processus de l'élection doit fournir des moyens de préserver et de détecter toute manipulation des données de configuration de l'élection utilisées pour organiser l'élection.

2.2.19 INTÉGRITÉ DES BULLETINS DE VOTE

Le processus de l'élection doit fournir des moyens de préserver et de détecter toute manipulation des bulletins de vote déposés par un votant admissible.

2.3 EXIGENCES NON FONCTIONNELLES

2.3.1 DÉCHIFFREMENT DES VOTES

a. Le système a recours au conseil de gestion du vote en réseau pour le déchiffrement des votes déposés.

b. Le système utilise un schéma cryptographique à seuil des membres du conseil de gestion du vote en réseau pour extraire les clés permettant le déchiffrement des votes.

c. Il doit être impossible pour un membre ou un certain nombre de membres sous le seuil d'extraire la clé de déchiffrement de l'élection.

d. Le système doit prendre en charge le recours à des dispositifs inviolables (p. ex., des cartes à puce intelligentes protégées par un NIP) pour archiver l'information dont a besoin chaque membre du conseil de gestion du vote en réseau pour extraire la clé de déchiffrement de l'élection.

e. Le seuil repose sur une méthode cryptographique (p. ex., le plan de partage secret).

f. La clé de déchiffrement est détruite par le schéma à seuil et n'existe pas tant qu'elle n'est pas reconstruite par les membres du conseil de gestion du vote en réseau à la fin de l'élection.

2.3.2 DISPONIBILITÉ ET RENDEMENT DU SERVICE

Explication des ententes sur les niveaux de service requis sur le plan de la disponibilité et du rendement

a. Le système de vote doit être disponible 99,95 % du temps au cours de la période de vote.

b. Le système de vote doit pouvoir prendre en charge simultanément au moins 100 votants qui votent par ordinateur et, en parallèle, 100 votants qui votent par téléphone.

c. Les terminaux de votation situés dans les bureaux de scrutin doivent pouvoir fonctionner durant toute la période de vote.

d. Le déchiffrement et la compilation des bulletins de vote doivent pouvoir fournir des résultats en moins de 30 minutes sur un nombre de votes pouvant atteindre 50 000 votes.

2.3.3 EXIGENCES EN MATIÈRE D'HÉBERGEMENT APPLICABLES AU SYSTÈME DE VOTE EN RÉSEAU

Cette section renferme les exigences en matière d'hébergement du système de vote dans l'infrastructure fournie par élections Ontario.

a. Élections Ontario fournira l'infrastructure d'hébergement du système de vote en réseau, ainsi que la connectivité internet.

b. Le fournisseur de service doit décrire ses besoins en matériel, logiciel COTS, réseautage et dispositifs de sécurité pour assurer la disponibilité et la performance nécessaires.

c. Élections Ontario sera chargé de fournir le matériel, le logiciel COTS, le réseautage et les dispositifs de sécurité, de même que des services de surveillance en tout temps jusqu'au niveau du système d'exploitation.

d. Le fournisseur de service est chargé de déployer le logiciel requis et le système d'exploitation (y compris les serveurs de l'application, les bases de données, etc.), ainsi que la configuration et le renforcement du système d'exploitation.

2.3.4 EXIGENCES APPLICABLES À LA RÉPONSE VOCALE INTERACTIVE

Cette section renferme les exigences en matière d'interface avec le système RVI fourni par élections Ontario.

a. Le système de vote doit utiliser le logiciel de RVI et les installations fournis par élections Ontario.

b. Le fournisseur de service doit décrire ses besoins en matériel, logiciel COTS, réseautage et dispositifs de sécurité pour faire interagir le logiciel de VRI d'Élections Ontario avec le système de vote et ainsi obtenir la disponibilité et la performance nécessaires.

c. Élections Ontario sera chargé de fournir le matériel, le logiciel COTS, le réseautage et les dispositifs de sécurité, de même que des services de surveillance en tout temps jusqu'au niveau du système d'exploitation.

d. Élections Ontario fournira le nombre nécessaire de lignes téléphoniques.

e. Le fournisseur de service est chargé de déployer le logiciel requis et le système d'exploitation (y compris les serveurs de l'application, les bases de données, etc.), ainsi que de la configuration et du renforcement du système d'exploitation.

2.3.5 SYSTÈME ISOLÉ DE DÉCHIFFREMENT ET DE COMPILATION

Cette section expose les exigences du système isolé qui est utilisé pour la configuration de l'élection et le déchiffrement et la compilation définitifs.

a. Les composantes du système de vote utilisé pour configurer l'élection et pour déchiffrer et compiler les bulletins de vote doivent fonctionner dans un environnement isolé composé d'un ou plusieurs serveurs/ordinateurs.

b. Le fournisseur de service doit décrire ses besoins en matériel et en logiciel COTS pour obtenir la disponibilité et la performance nécessaires.

c. Élections Ontario sera chargé de fournir le matériel et le logiciel COTS convenus.

d. Le fournisseur de service est chargé de déployer le logiciel requis et le système d'exploitation (y compris les serveurs de l'application, les bases de données, etc.) et de configurer et renforcer le système d'exploitation.

e. Le fournisseur de service doit également décrire ses besoins en échange de données entre le système isolé et les serveurs de l'élection situés dans l'environnement hébergé. Élections Ontario fournira l'accès internet nécessaire.

2.3.6 EXIGENCES EN MATIÈRE D'INFRASTRUCTURE DES BUREAUX DE VOTE

Cette section énonce les exigences relatives au déploiement des terminaux de votation dans les bureaux de vote.

a. Élections Ontario fournira l'infrastructure technologique nécessaire pour les éléments du système de vote en réseau qui sont déployés dans les bureaux de vote, ainsi que la connectivité à internet et aux lignes téléphoniques.

b. Le fournisseur de service doit décrire ses besoins en matériel, périphériques d'accessibilité, logiciel COTS, réseautage et dispositifs de sécurité pour assurer la disponibilité et la performance nécessaires. Fournir des estimations pour les éléments de sauvegarde.

c. Élections Ontario sera chargé de fournir le matériel, le logiciel COTS, le réseautage et les dispositifs de sécurité convenus, ainsi que le soutien technique.

d. Le fournisseur de service est chargé de déployer le logiciel requis en plus du système d'exploitation, de configurer et renforcer le système d'exploitation, et de configurer des périphériques d'accessibilité.

2.3.7 VARIABILITÉ

Exigences liées à la variabilité du système

a. Le système devrait être en mesure de prendre des élections en charge pour des dizaines de millions de votants facilement et de manière économique.

b. Le système doit permettre d'ajouter de nouvelles composantes sans avoir à mettre fin au service, p. ex. pour prendre en charge un plus grand nombre de votants.

2.3.8 SOUPLESSE

Exigences liées à la souplesse du système

a. Le système doit pouvoir prendre en charge toutes les caractéristiques du processus électoral de l'Ontario.

b. Plusieurs éléments du système doivent être adaptables, tels que l'aspect et la convivialité, la langue, les pages d'aide et d'information, à la suite des exigences d'élections Ontario.

c. Le système doit être en mesure de prendre en charge parallèlement deux modes de scrutin différents : le premier s'appuie sur les ordinateurs, et l'autre se fonde sur la voix (téléphones).

d. Le système doit pouvoir fonctionner parallèlement dans deux environnements différents : sur site (à partir des bureaux de vote) et à distance (de n'importe où).

e. Le système doit prendre en charge plusieurs mécanismes d'authentification des votants. Ces mécanismes devraient pouvoir fonctionner parallèlement, afin que le taux de participation puisse être à son maximum. Les mécanismes choisis dans le cadre de ce projet sont l'authentification sur site basée sur des id physiques et l'authentification à distance basée sur les justificatifs d'identité du votant (NIP).

f. Les outils de gestion du système doivent être adaptables aux exigences d'élections Ontario, telles que la capacité d'avoir accès au taux de participation en temps réel, de vérifier le système, ou d'annuler ou de révoquer certains votes à la suite des procédures convenues.

g. Le système doit permettre des intégrations faciles aux systèmes actuels d'élections Ontario, dont son système de gestion des élections.

2.3.9 NORMES TECHNIQUES

a. Le fournisseur de système doit inclure une liste de normes de chiffrement et de sécurité respectées par le système de vote proposé.

b. Les algorithmes cryptographiques utilisés doivent être fondés sur des normes internationales et ouvertes.

c. Le système de vote devrait être compatible avec Election Markup Language (EML).

2.3.10 EXEMPT DE CONFLITS EN PI

Le fournisseur de système doit garantir que la solution ne présente pas de conflits en matière de propriété intellectuelle avec des tiers.

APPENDICE B : LISTE DES RISQUES

Cet appendice donne une liste détaillée des risques recensés dans le contexte des scénarios retenus :

- risques en matière de sécurité;
- risques liés aux opérations;
- risques pour le votant.

2.4 RISQUES EN MATIÈRE DE SÉCURITÉ

Les risques en matière de sécurité qui doivent être gérés et atténués peuvent être subdivisés en quatre catégories :

- vie privée et confidentialité du votant;
- intégrité du vote et exactitude des résultats;
- disponibilité du système électoral;
- vérifiabilité.

Vie privée et confidentialité du votant

RISQUES	ATTAQUES POSSIBLES
Mise en péril de la confidentialité du votant Un pirate pourrait violer la vie privée du votant, relier un votant et ses options de vote et par conséquent violer le caractère secret du vote.	• Un pirate externe pourrait intercepter les communications entre le terminal de votation et les serveurs de l'élection pour accéder au contenu du vote. • Un administrateur de système ayant accès aux serveurs de l'élection pourrait avoir accès à l'ensemble de l'urne qui contient tous les votes. • Un administrateur de système d'une composante intermédiaire de l'infrastructure (plateforme VRI, serveurs intermédiaires, etc) pourrait avoir accès aux votes en transit (renfermant les options de vote retenues par les votants). • Un logiciel malveillant exploité dans des terminaux de votation peut avoir accès aux options de vote retenues par les votants. • Un responsable de l'élection pourrait avoir accès aux votes au cours du processus d'établissement des résultats

RISQUES	ATTAQUES POSSIBLES
	et identifier les options de vote de chaque votant.
Publication de résultats intermédiaires non autorisés Les résultats intermédiaires pourraient être divulgués avant la clôture de l'élection, ce qui influencerait les votants qui n'ont pas encore exercé leur droit de vote.	• Quiconque ayant accès aux serveurs de l'élection pourrait calculer et publier les résultats intermédiaires. • Quiconque ayant accès à la composante de l'infrastructure intermédiaire (plateforme RVI, serveurs intermédiaires, etc) pourrait avoir accès aux votes en transit, et calculer et publier des résultats intermédiaires. • Un responsable de l'élection pourrait effectuer le processus d'établissement des résultats avant la fin de l'élection, pour obtenir des résultats intermédiaires.

INTÉGRITÉ DU VOTE ET EXACTITUDE DES RÉSULTATS

RISQUES	ATTAQUES POSSIBLES
Remplissage des urnes Un pirate peut tenter d'ajouter à l'urne des votes de votants qui n'ont pas participé au processus de vote.	• Quiconque ayant accès aux serveurs de l'élection pourrait avoir accès à l'urne, et tenter de déposer des votes directement dans la base de données. • Un pirate interne ou externe pourrait déposer des votes à partir d'un serveur intermédiaire de la solution de vote (et ainsi éviter les filtres précédents). • Avant le début de l'élection, une personne pourrait charger une urne qui n'est pas vide dans les serveurs de l'élection. • Un responsable de l'élection pourrait ajouter des votes contrefaits pendant le processus de compilation.
Vote sous la contrainte et achat de votes Un particulier ou une organisation pourrait	• Un votant pourrait exprimer un suffrage sous la surveillance d'une personne

RISQUES	ATTAQUES POSSIBLES
corrompre un votant ou le contraindre à voter pour un candidat précis.	qui achète des votes ou exerce de la contrainte. • Un votant peut montrer ses options de vote à une personne qui achète des votes ou fait voter sous la contrainte.
Modification du vote Le contenu du vote pourrait être changé de manière à modifier les résultats de l'élection.	• Un logiciel malveillant utilisé dans les terminaux de votation peut modifier les options de vote retenues par un votant. • Un pirate externe pourrait intercepter les communications entre le terminal de votation et le serveur de l'élection, et modifier un vote. • Un administrateur de système ou un pirate de l'extérieur pourrait avoir directement accès à l'urne et modifier le contenu d'un vote valide. • Au cours du processus de compilation, un responsable de l'élection pourrait remplacer des votes valides par des votes contrefaits, voire remplacer toute l'urne par une urne contrefaite.
Suppression de vote Un pirate pourrait tenter de supprimer des votes valides de l'urne.	• Un administrateur de système ou un pirate externe pourrait être en mesure d'avoir directement accès à l'urne et de supprimer un vote valide. • Un pirate externe pourrait intercepter le vote entre le terminal de votation et le serveur de l'élection, ce qui laisserait croire au votant que le bulletin de vote a été déposé avec succès. • Au cours du processus de compilation, un responsable de l'élection pourrait supprimer des votes.
Incertitude du votant quant au bulletin de vote déposé	• Le votant pourrait éprouver le sentiment que son vote n'a pas été

RISQUES	ATTAQUES POSSIBLES
Un votant ne dispose pas d'une façon de vérifier la réception et le dépouillement corrects de son vote. Par conséquent, le votant pourrait éprouver un sentiment négatif au sujet du processus de vote.	déposé adéquatement. • Le votant pourrait avoir le sentiment que son vote ne s'est pas rendu jusqu'à l'urne.
Modification des résultats du scrutin Les résultats de l'élection peuvent être modifiés sans avoir accès aux votes ou à l'urne, en manipulant le résultat ou le dépouillement.	• Un travailleur en place malveillant pourrait modifier les résultats du scrutin au cours du processus de dépouillement. • L'application de vote pourrait modifier les résultats du scrutin pendant le processus de dépouillement. • Un pirate (externe ou interne) pourrait modifier les résultats de l'élection après le processus de dépouillement. • Un pirate (externe ou interne) pourrait modifier les résultats d'élection publiés.

Disponibilité du système électoral

RISQUES	ATTAQUES POSSIBLES
Boycott de l'élection-refus de service Un pirate pourrait perturber la disponibilité du mode de scrutin en effectuant une attaque entraînant un refus de service.	• Le système de vote pourrait être inondé de fausses demandes de voter pour surcharger le système et empêcher que des votes valides soient traités. • Les serveurs de l'élection pourraient être inondés de demandes malveillantes pour provoquer une défaillance du serveur.
Authenticité du votant	
Usurpation de l'identité du votant Un votant ou un pirate pourrait tenter de déposer un vote au nom d'une autre personne.	• Un pirate pourrait voler les justificatifs d'identité d'un votant et déposer un vote valide au nom du votant autorisé. • Un pirate pourrait voler tous les justificatifs d'identité du votant dans les serveurs de l'élection, et transmettre massivement des votes valides au nom des votants autorisés. • Un pirate pourrait tenter d'obtenir des justificatifs d'identité du votant valides (en les devinant, ou par des attaques en force) et de déposer un vote valide au nom de votants autorisés.
Les votants non autorisés qui votent Les votants non admissibles pourraient tenter d'exprimer un suffrage lors d'une élection en particulier.	• Un votant non admissible pourrait tenter de déposer un vote. • Un pirate pourrait tenter – à titre de votant non admissible – de déposer un vote en contournant le processus d'authentification. • Un votant pourrait obtenir un accès au système pour déposer un vote dans une élection en particulier, et tenter de déposer un vote lors d'une élection pour

RISQUES	ATTAQUES POSSIBLES
	laquelle il n'est pas autorisé à voter. • Un pirate pourrait tenter de modifier la liste électorale gérée par l'application de vote, pour être inclus comme votant admissible.

Vérifiabilité

RISQUES	ATTAQUES POSSIBLES
Vérifiabilité inexacte Une traçabilité insuffisante de l'élection ou des données de vérification faciles à altérer peuvent permettre aux pirates de cacher un comportement interdit.	• Les systèmes de vote n'enregistrent pas assez de données de vérification pour vérifier le processus de vote ou de compilation. • Les systèmes de vote enregistrent de fausses données de vérification pour démontrer qu'une élection frauduleuse est valide. • Les données de vérification pourraient être modifiées par un pirate – sans que ce geste soit repéré – pour démontrer qu'une élection frauduleuse était considérée valide, ou pour révoquer une élection valide.

2.5 RISQUES LIÉS AUX OPÉRATIONS

Cette section présente une série de risques liés aux opérations rattachés au système de vote en réseau. Les risques génériques qui s'appliquent à un projet régulier ne sont pas compris dans cette présentation.

Risques dans le bureau de vote

RISQUE	ATTAQUE POSSIBLE
La technologie SVR requise ne fonctionne pas dans les bureaux de vote Les terminaux utilisés pour voter et (ou) pour	• Un processus logistique complexe pourrait occasionner des retards dans la livraison des composantes requises aux bureaux de vote.

RISQUE	ATTAQUE POSSIBLE
gérer la liste des votants ne fonctionnent pas et ne peuvent être utilisés dans les bureaux de vote.	• Un vice de fonctionnement du logiciel ou du matériel rend le SVR inopérable. • Les problèmes de connectivité nuisent à la technologie du SVR dans les bureaux de vote pour établir la connexion avec le centre de données. Ce problème de connectivité pourrait aller d'une interruption totale à des coupures sporadiques mais constantes, qui rendent le système inopérable. • Des pannes de courant pourraient rendre le SVR indisponible dans les bureaux de vote. • Le sabotage des installations du bureau de vote (p. ex., une porte qui ne s'ouvre pas, un incendie, etc.) et (ou) des composantes du SVR (retrait de composantes requises comme l'écran et autres) pourrait entraîner l'indisponibilité du SVR. • le montage incorrect causé par une livraison tardive, l'emploi de personnel sous-qualifié, etc., pourrait entraîner une installation incorrecte du SVR au bureau de vote, ce qui rendrait le fonctionnement du SVR de marginal à inexistant.
Les responsables de l'élection utilisent le SVR de manière incorrecte aux bureaux de vote. Les responsables de l'élection chargés d'exploiter les différentes composantes du SVR sont incapables de l'exploiter correctement.	• Une formation insuffisante de ce personnel, qui n'est pas détectée à temps, pourrait occasionner une exploitation incorrecte du SVR. L'impact pourrait comprendre une perception negative d'ÉO et du SVR et la violation des principes électoraux. • Soutien insuffisant fourni aux responsables de l'élection. Pourrait être causé par une équipe de soutien de taille insuffisante et inadéquatement formée. Pourrait entraîner un règlement incorrect des problèmes des responsables de l'élection au niveau de l'exploitation du SVR. La mauvaise

RISQUE	ATTAQUE POSSIBLE
	utilisation par mégarde du système qui en résulte pourrait faire en sorte que les principes électoraux soient touchés. • Les interfaces du SVR pour les responsables de l'élection ne sont pas conviviales, ce qui crée de la confusion chez les responsables de l'élection pendant l'exploitation des systèmes et (ou) rend leur travail plus difficile et (ou) plus lent. • L'insuffisance de la formation du personnel de relève pourrait entraîner l'emploi de responsables de l'élection qui n'ont pas de formation adéquate dans l'utilisation du SVR. Ce besoin pourrait se présenter en situation de grève, de maladie, de catastrophe naturelle, etc. qui pourrait affecter un certain nombre de responsables de l'élection en même temps.

Risques au niveau du centre des données

RISQUE	ATTAQUE POSSIBLE
Il manque des composantes du SVR Il manque certaines composantes centrales du SVR qui sont nécessaires, qu'il s'agisse du matériel, du logiciel, ou d'autres produits de communications.	• Retards dans la livraison des éléments requis au centre de données. • Sabotage de certaines composantes par des pirates internes ou externes.
Le SVR ne fonctionne pas bien Certaines composantes centrales du SVR qui sont nécessaires, qu'il s'agisse du matériel, de logiciels ou de produits de communications connexes, ne fonctionnent pas correctement, par eux-mêmes ou en interaction avec d'autres éléments.	• Le sabotage de la configuration d'éléments du centre de données (externe ou interne) affecterait la disponibilité de l'ensemble du SVR. • Le montage incorrect causé par une livraison tardive, l'emploi de personnel sous-qualifié, la complexité inhérente des déploiements au centre de données, etc. Pourrait entraîner une organisation incorrecte du SVR dans ses installations

RISQUE	ATTAQUE POSSIBLE
	centrales, ce qui affecterait l'ensemble de l'élection. • Une intégration faite incorrectement entre les différentes composantes (p. ex. En raison de mises en œuvre incorrectes, d'exigences inappropriées, de problèmes de connectivité…) pourrait affecter l'élection.
Les techniciens exploitent le SVR incorrectement. les techniciens du centre de données chargés de surveiller le fonctionnement correct de l'infrastructure du SVR se sont comportés de manière incorrecte (intentionnellement ou non).	• Une connaissance insuffisante des systèmes essentiels à la mission pourrait entraîner un fonctionnement incorrect du centre de données, ce qui affecterait la disponibilité du SVR. • Une formation insuffisante portant sur le système déployé pourrait occasionner son fonctionnement et son entretien incorrects, ce qui affecterait la disponibilité et la vérifiabilité du SVR. • La corruption ou la contrainte de techniciens du centre de données pourrait les amener à faire fonctionner incorrectement le SVR à dessein, pour influer sur le résultat de l'élection et (ou) sur son image publique. • Une définition inadéquate des procédures de fonctionnement du centre de données requises pourrait entraîner une gestion incorrecte du système et des décisions incorrectes lorsque surviennent des situations inattendues.

Risques pour le bureau central d'ÉO

RISQUE	ATTAQUE POSSIBLE
Les composantes requises du SVR ne sont pas opérationnelles. Les composantes du SVR qui sont exploitées par ÉO ne sont pas opérationnelles lorsqu'elles sont nécessaires, ce qui affecte l'ensemble de l'élection.	• Des retards au niveau de la logistique et de l'approvisionnement pourraient faire en sorte qu'il manque des éléments requis pour exploiter le SVR. • Une défaillance du logiciel ou du matériel rend le SVR inapte à fonctionner. • Des problèmes de connectivité nuisent à la technologie du SVR au bureau central sur le plan du branchement au centre de données. Ce problème de connectivité pourrait aller d'une interruption totale à des coupures sporadiques mais constantes, qui rendent le système inopérable. • Des pannes de courant pourraient rendre le SVR indisponible au bureau central. • Le sabotage des installations du bureau central (p. ex., une porte qui ne s'ouvre pas, un incendie, etc.) et (ou) des composantes du SVR (retrait de composantes requises comme l'écran et autres) pourrait entraîner l'indisponibilité du SVR. • Le montage incorrect causé par une livraison tardive, l'emploi de personnel sous-qualifié, etc., pourrait entraîner une installation incorrecte du SVR au bureau central, ce qui rendrait le fonctionnement du SVR de marginal à inexistant.
Disponibilité des données électorales Certaines données critiques qui sont nécessaires pour configurer/exploiter le SVR sont manquantes ou ne sont pas disponibles à temps.	• Les données ne correspondent pas au format correct qui a été défini avant les élections, ce qui affecte la capacité du SVR de les traiter automatiquement et peut nécessiter une opération manuelle, qui pourrait affecter l'intégrité de l'élection, introduire des erreurs manuelles dans l'élection (p. ex. des candidats manquants, etc.) et (ou) des retards. • Les données nécessaires sont disponibles trop tardivement pour le SVR, ce qui retarde l'ouverture de la période de vote

RISQUE	ATTAQUE POSSIBLE
	électronique. • Les ensembles de données sont incomplets et il y manque de l'information, ce qui pourrait affecter l'élection, et par conséquent engendrer des retards et (ou) nécessiter des opérations manuelles pouvant introduire des erreurs.
Exploitation incorrecte du SVR Les techniciens chargés d'exploiter les composantes du SVR qui se trouvent au bureau central ne les exploitent pas correctement (intentionnellement ou non).	• Une connaissance insuffisante des systèmes essentiels à la mission pourrait entraîner un fonctionnement incorrect du SVR au bureau central, ce qui affecte la configuration du SVR et retarde le début de la période de vote et (ou) la remise finale des résultats. • Une formation insuffisante portant sur le système déployé pourrait occasionner son fonctionnement et son entretien incorrects, ce qui affecterait la vérifiabilité et le rendement du SVR. • la corruption ou la contrainte de techniciens du bureau central pourrait les amener à faire fonctionner incorrectement le SVR à dessein, pour influer sur le résultat de l'élection et (ou) sur son image publique. • une définition inadéquate des procédures de fonctionnement des composantes du SVR au bureau central requises pourrait entraîner une exploitation incorrecte du système à l'égard des opérations essentielles et des décisions incorrectes lorsque surviennent des situations inattendues.

RISQUES TOUCHANT LE BUREAU D'ASSISTANCE D'ÉO

RISQUE	ATTAQUE POSSIBLE
Soutien inapproprié aux responsables de l'élection	• Formation insuffisante donnée au personnel du bureau d'assistance.

Le bureau d'assistance n'est pas en mesure d'offrir du soutien convenable aux responsables de l'élection qui utilisent le SVR aux bureaux de vote.	• Personnel de relève insuffisamment formé pour s'occuper des situations pour lesquelles le personnel formé n'est pas disponible pour répondre aux besoins. • Le personnel de soutien de deuxième et de troisième niveau est inapproprié et insuffisant pour aider efficacement les membres du personnel de soutien de premier niveau. • Les procédures et les guides d'assistance qui ne sont pas assez définis ne permettent pas au personnel du bureau d'assistance d'aider efficacement les responsables de l'élection, qui doivent s'occuper de problèmes de base.
Soutien inapproprié aux votants Le bureau d'assistance ne peut fournir de soutien convenable aux votants qui utilisent le SVR à distance.	• Formation insuffisante donnée au personnel du bureau d'assistance. • Personnel de relève insuffisamment formé pour s'occuper des situations pour lesquelles le personnel formé n'est pas disponible pour répondre aux besoins. • Le personnel de soutien de deuxième et de troisième niveau est inapproprié et insuffisant pour aider efficacement les membres du personnel de soutien de premier niveau. • Les procédures et les guides d'assistance qui ne sont pas assez définis ne permettent pas au personnel du bureau d'assistance d'aider efficacement les votants, qui doivent s'occuper de problèmes de base.

2.6 RISQUES LIÉS AUX VOTANTS

Les risques expliqués ci-après sont liés aux votants, et englobent leur interaction avec le svr à divers stades, leurs perceptions du système en particulier, et du vote en réseau en général.

Interaction avec le système de vote en réseau

RISQUE GÉNÉRIQUE	MENACES
Le SVR n'est pas convivial L'interaction avec le SVR n'est ni facile ni intuitive pour les votants, ce qui contrecarre des tentatives de voter et nuit à la perception qu'a le public d'ÉO et du SVR.	• Des interfaces utilisateur inutilisables qui nuisent à la capacité des votants (ou à un sous-groupe de votants, p. ex. Les citoyens âgés) d'exprimer un suffrage de façon satisfaisante sans demander d'aide ou consacrer à leur geste plus de temps que prévu. • Certaines langues utilisées fréquemment par certains groupes de votants ne sont pas comprises dans l'interface de vote du SVR, ce qui se répercute sur la capacité de voter de ces votants. • La dépendance inhérente à l'égard d'un logiciel tiers (p. ex. Les navigateurs web) face à la création de l'interface utilisateur de vote pourrait faire en sorte que certaines versions affichent bizarrement les bulletins de vote (p. ex. Contenu déplacé, options dissimulées), ce qui a une incidence sur l'expérience de voter. • Les contraintes imposées par la loi qui touchent la conception des bulletins de vote limitent les options de facilité d'utilisation au niveau de la conception du bulletin de vote électronique. • L'insuffisance de renseignements appropriés pour aider les votants peut nuire aux votants qui tentent de déposer un vote par voie électronique. • Les votants qui utilisent de vieux ordinateurs qui ne sont pas compatibles avec le SVR. Si les votants n'ont pas clairement accès à l'information sur l'incompatibilité, les tentatives de voter pourraient se révéler frustrantes.

RISQUE GÉNÉRIQUE	MENACES
	• Des bulletins de vote et (ou) des procédures complexes qui doivent être repris dans le SVR nuisent à la capacité des votants de voter intuitivement sans soutien externe, ce qui se répercute sur leur perception du SVR en particulier et d'ÉO en général.
Le SVR comporte des éléments d'accessibilité insuffisants Le système SVR comporte des éléments d'accessibilité insuffisants ce qui nuit à certains votants lorsqu'ils tentent de voter par eux-mêmes, sans aide externe.	• Il manque des éléments d'accessibilité, qui devraient s'appliquer à certains types de handicaps, ce qui nuit aux votants qui ont ces handicaps. • Les éléments d'accessibilité pris en charge par le SVR ne sont pas appliqués correctement, ou sont appliqués d'une façon non-conviviale pour les votants ainsi handicapés (p. ex. Ceux qui comptent sur un clavier en braille alors qu'une minorité de votants aveugles connaissent le braille). • Les votants se servent de certains accessoires d'accessibilité qui ne sont pas pris en charge par le SVR. • Les contraintes imposées par la loi qui touchent la conception des bulletins de vote limitent les options d'accessibilité au niveau de la conception du bulletin de vote électronique.
Processus d'inscription trop lourd Le processus d'inscription requis pour utiliser le mode de vote en réseau est trop complexe pour y faire participer une masse critique de votants.	• Le processus exige des étapes trop nombreuses et (ou) trop complexes, • ce qui atténue la volonté des votants de participer. • Le processus exige que les votants aient accès à certains renseignements personnels qui ne leur sont pas accessibles. • Les données liées aux votants qui sont nécessaires pour exécuter le processus d'inscription comportent trop d'erreurs, ce qui affecte le résultat. • Le processus s'en remet à des tiers, comme le service postal, qui peut être à l'origine d'erreurs (p. ex. Livraison au mauvais destinataire).

PERCEPTION DU VOTANT

risque générique	Menace s
Méfiance des votants envers le SVR Les votants peuvent se méfier du SVR et croire qu'il ne respecte pas les principes qui doivent être suivis dans le cadre d'un processus électoral. Cette situation amènera les votants à s'insurger contre le vote électronique et fera diminuer le nombre de cybervotants.	• Des lacunes évidentes en matière de sécurité (techniques et (ou) procédurales) affectent la confiance du votant à l'égard du SVR et de l'élection. • Les activistes qui sont contre le vote électronique font très vigoureusement campagne contre le SVR et (ou) l'initiative de vote en réseau d'ÉO, et retiennent ainsi l'attention des médias et des citoyens. • Les duperies et les canulars sur le SVR non découverts rendent les votants méfiants à l'égard du SVR. • La méfiance naturelle des votants à l'endroit des technologies affecte leur approche initiale à l'égard du SVR.
Les votants qui trompent le SVR Certains votants peuvent tenter de tromper le SVR et croire à tort qu'ils peuvent le faire.	• Des votants croient qu'ils ont pu voter deux fois ou plus et que ces différents votes seront dépouillés. • Des votants prétendent n'avoir jamais voté auparavant, en faisant valoir que le SVR est vicié, pour tenter de voter de nouveau dans un bureau de vote, voire à distance. • Des votants tentent intentionnellement d'avoir un effet sur le SVR en votant à distance, en utilisant des trucs tels que reculer sur l'écran avec le navigateur, et tenter de déposer un nouveau bulletin de vote, etc.
Le votant ignore l'existence d'un nouveau mode de scrutin La majorité des votants approchés pour utiliser le SVR ne sont pas au courant de cette nouvelle possibilité, ou l'apprennent trop tard.	• Le plan de diffusion est inadéquat, et ne se rend pas bien jusqu'aux votants visés. • Les activités de diffusion sont exécutées trop tardivement. • Activités de diffusion insuffisantes.

APPENDICE C : RENSEIGNEMENTS SUR LES CONSULTATIONS DES PARTIES PRENANTES

À la réunion du CCA tenue à Toronto le 26 janvier, les questions suivantes ont été présentées aux membres du comité qui y ont répondu en tour de table :

1. Supposons qu'Élections Ontario désirait inviter des électeurs handicapés seulement pour prendre part à notre essai de fonctionnement du vote en réseau. Comment est-ce réalisable? Qu'est-ce qu'Élections Ontario devrait prendre en compte au sujet des tentatives de chercher à confirmer qui est un électeur handicapé et qui ne l'est pas?
2. Veuillez traiter de l'importance des caractéristiques suivantes, en les classant si possible et en expliquant votre classement :
   - confidentialité
   - confiance à l'égard du système/de la sécurité
   - commodité et facilité d'utilisation
   - indépendance personnelle
   - autre
3. Après réflexion sur les divers modes de vote en réseau (vote par internet, vote par téléphone, ou autres options comme les téléphones intelligents ou les messages texte), veuillez traiter des avantages et des inconvénients de chaque option du point de vue des électeurs handicapés.
4. Quelle est la meilleure façon, pour le comité, d'appuyer le projet de vote en réseau jusqu'en 2012 (p. ex., participer à un essai d'acceptation par l'utilisateur, etc.)?
5. Qui d'autre chez les électeurs handicapés devrions-nous consulter au sujet du vote en réseau maintenant ou lors des étapes à venir?
6. Quelles technologies d'aide au vote ou autres mesures de soutien pourraient devoir être utilisées pour rendre possible le vote en réseau pour les électeurs handicapés (p. ex., un site web d'ÉO accessible pour les électeurs non voyants; des instructions conviviales pour les personnes ayant un handicap cognitif; etc.)? (Est-ce que certains besoins d'électeurs handicapés nécessiteront une solution de vote en réseau différente de celle du grand public?)

APPENDICE D : FACTEURS D'ACCESSIBILITÉ POUR LE CONTENU WEB ET VRI

CONTEXTE

La direction générale de l'accessibilité pour l'Ontario a rédigé un règlement[19] qui exigera que les sites web du gouvernement se conforment graduellement aux directives pour l'accessibilité aux contenus web de niveau AA (DACW 2.0) à compter de janvier 2012. Il ne prévoit pas de normes précises sur l'accessibilité des systèmes de réponse vocale interactive (RVI).

FACTEURS D'ACCESSIBILITÉ AU WEB

Les DACW 2.0, publiées par W3C, sont un ensemble détaillé de lignes directrices sur le contenu des sites web. Ces directives ont pour but de rendre le contenu accessible à tous les utilisateurs, essentiellement les utilisateurs handicapés. Quoique certaines des pratiques de conception qui appuient une expérience fondée sur l'accessibilité soient spécifiques, bon nombre de ces pratiques sont cohérentes avec une bonne conception Web. À un niveau élevé, les DACW 2.0 précisent ce qui suit :

DIRECTIVES DACW

Le contenu doit être **utilisable**, en ce sens qu'il doit être facile à lire et que des solutions de rechange textuelles sont fournies pour le contenu vidéo ou audio.

Le contenu doit être **fonctionnel**, ce qui signifie que la fonctionnalité est disponible à partir du clavier, que les utilisateurs disposent d'assez de temps pour lire et comprendre le contenu (y compris les facteurs de sessions authentifiées), et que les utilisateurs ont de nombreuses façons de localiser leur position dans le cadre de la navigation sur un site Web.

Le contenu doit être **compréhensible**, c'est-à-dire qu'il est lisible et exempt de jargon ou d'abréviations superflues, qu'il ne nécessite pas de capacité de lecture excédant le début des études secondaires, et que les pages sont prévisibles sur le plan de l'orientation et du contexte.

Le contenu doit être **compatible**, ce qui signifie qu'il peut être interprété par des technologies d'aide au vote et, plus important encore, que HTML (descripteurs, attributs ID) est mis en œuvre conformément aux spécifications.

LECTEURS D'ÉCRAN

Les utilisateurs qui ont un handicap visuel peuvent s'en remettre à des lecteurs d'écran pour accéder à des pages web. Ces outils d'aide interprètent le code HTML de la page et le reproduisent sous forme de discours. Il existe de nombreuses façons grâce auxquelles les pages web peuvent aider un lecteur d'écran à présenter une interprétation exacte et compréhensible d'une page web. L'utilisation de tableaux à des fins de mise en page, par exemple, peut faire en sorte qu'un lecteur d'écran présente du contenu dans un ordre incorrect ou qui porte à confusion et devrait être évitée.

Outre les facteurs à prendre en compte pour les utilisateurs aveugles, les utilisateurs daltoniens peuvent éprouver de la difficulté à naviguer sur des sites qui s'en remettent à certaines couleurs pour présenter du contenu ou de la signification, et les utilisateurs ayant une faible vision devraient pouvoir augmenter la dimension du texte ou choisir un affichage à contraste élevé. Les utilisateurs qui ont un handicap moteur pourraient avoir besoin d'utiliser le clavier plutôt qu'une souris pour naviguer, ce qui fait que la conception du site pourrait devoir prendre en charge la navigation et la sélection fondées sur le clavier.

FACTEURS D'ACCESSIBILITÉ RVI

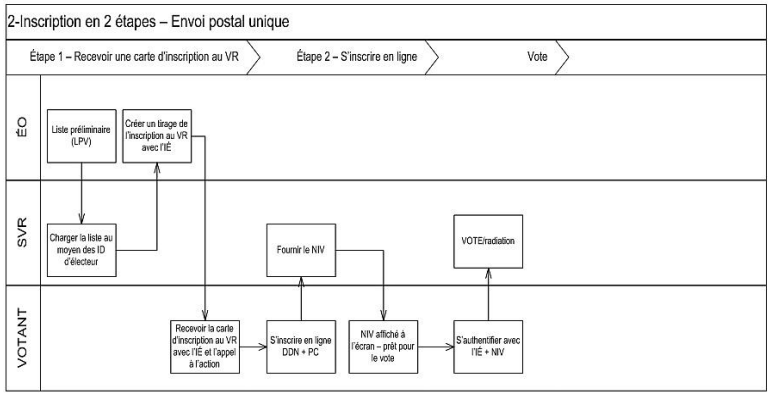
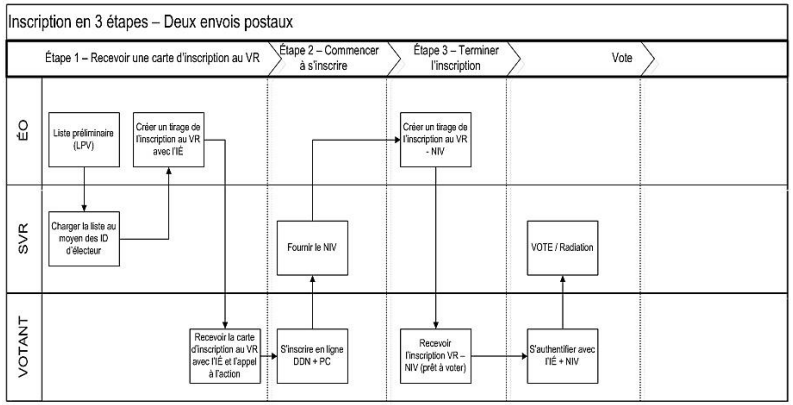
Pour chaque utilisateur, la facilité d'utilisation de l'interface de RVI repose sur la capacité de l'utilisateur d'entendre et de saisir les menus et le reste du contenu enregistré. La facilité d'utilisation dépend en outre de la capacité de l'utilisateur de faire des choix à partir des options de menu fournies. Les facteurs qui affectent l'accessibilité et la facilité d'utilisation de ces mesures englobent :

- qualité sonore (dont la clarté du discours enregistré et un fonds calme),
- vitesse du contenu et capacité d'ajuster la vitesse de lecture,
- capacité d'ajuster le niveau du volume de lecture,
- capacité de répéter ou de rebobiner les menus et d'autres contenus, ainsi que les sélections de l'utilisateur;
- durée du délai d'inactivité imposé dans les sélections de l'utilisateur.

Ces facteurs de la facilité d'utilisation améliorent l'expérience générale de l'utilisateur ainsi que l'accessibilité pour les utilisateurs qui éprouvent de la difficulté à entendre ou à traiter le contenu, ainsi que pour ceux qui ont de la difficulté à faire des choix en raison d'un handicap visuel ou moteur. Bien que les utilisateurs aveugles soient en mesure d'obtenir de l'information par la voie sonore qui serait inaccessible sur un écran par présentation textuelle, le système RVI doit accorder assez de temps à l'utilisateur pour qu'il fasse un choix dans le menu.

L'accessibilité pour le malentendant peut être offerte par les mesures de contrôle de la facilité d'utilisation décrites précédemment, pourvu que le volume puisse être assez élevé. L'accès aux systèmes RVI pour les utilisateurs qui comptent sur le TTY exige que l'équipement des utilisateurs du TTY puisse produire des doubles tonalités multifréquences, ce qui constitue une restriction de certains appareils. Du point de vue de la facilité d'utilisation, le système RVI doit accorder assez de temps à l'utilisateur pour qu'il puisse indiquer un choix sans dépasser le temps imparti.

APPENDICE E : COMPARAISON DE L'AUTHENTIFICATION

	1	2
	Processus en 2 étapes – Envoi postal simple	***Processus en 3 étapes – Envoi postal double***
FLUX		
DESCRIPTION	• Deux étapes • Le système ou le votant peut générer un NIV/MOT de passe • Utilisé par d'autres administrations dans plusieurs élections (comme Genève depuis 2003)	• Trois étapes • Le système doit générer le NIV/MOT de passe • Utilisé par des municipalités de l'Ontario lors des élections de 2010 (Markham, Peterborough)
AVANTAGES	• vérifie l'identité du votant au moyen de méthodes multiples - résidence à l'adresse postale - preuve d'identité (DDN + PC) • le votant est prêt à voter immédiatement après avoir prouvé son identité en ligne • l'inscription peut se poursuivre tout au long du processus de vote - donne plus de souplesse aux votants	• le votant prouve son identité en utilisant seulement son adresse postale à sa résidence et sa DDN • atténuation apparente du risque d'usurpation d'identité par les parties prenantes • autres éléments dissuasifs qui s'appliquent au risque d'usurpation d'identité (il est plus difficile d'intercepter 2 objets de correspondance qu'un seul) • tous les votants seront traités de la même façon • légère amélioration à la sécurité : le fait de vérifier

	1 ***Processus en 2 étapes – Envoi postal simple***	2 ***Processus en 3 étapes – Envoi postal double***
	- accorde du temps pour le traitement des exceptions (électeurs sans PC) • processus simple = facilité d'adoption	deux fois l'identité au moyen de la même méthode (résidence à l'adresse postale) ajoute très peu de sécurité, mais peut ajouter une perception de sécurité accrue
INCONVÉN-IENTS	• la simplicité du processus peut donner lieu à une perception de sécurité affaiblie • les électeurs sans pc doivent être traités différemment - des options peuvent nécessiter des transactions physiques • - des options peuvent exiger que les votants envoient une preuve d'identité comme dans le cas des bulletins de vote spéciaux.	• temps écoulé plus long - période d'inscription plus courte / date limite plus rapprochée avant le début du scrutin par anticipation afin de prévoir du temps pour l'arrivée du 2e envoi postal - temps limité pour traiter les exceptions - le temps requis pour la livraison de la 2e carte diminuera l'adoption, en particulier pour les électeurs qui vivent dans des régions sans livraison à domicile • complexité accrue pour le votant et ÉO - volumes accrus des centres d'appels • augmentation des frais postaux / d'impression et des frais de personnel
RISQUES	• Risque d'usurpation d'identité de faible à moyen si quiconque a accès au courrier et au numéro de PC	• faible risque d'usurpation d'identité si quelqu'un a accès au courrier • la complexité du processus fera diminuer l'adoption / causera de la confusion • les retards de réception de la carte diminueront l'adoption
EXCEPTIONS	• si les votants n'ont pas de pc, ils peuvent prouver leur identité sur site au bureau du directeur de	• la perte de l'ID d'électeur nécessitera deux envois postaux supplémentaires, ce qui ajoutera au temps

	1	2
	Processus en 2 étapes – Envoi postal simple	***Processus en 3 étapes – Envoi postal double***
	scrutin ou en postant une preuve d'identité (plus de temps requis)	écoulé (recommencement du processus) • la perte d'un mot de passe nécessitera un troisième envoi postal, ce qui ajoutera au temps écoulé
SOLUTIONS DE RECHANGE	• les votants pourraient créer leurs propres mots de passe (sous réserve des règles relatives à la complexité) • le mot de passe pourrait être transmis par SMS • chaque utilisateur (ID d'électeur) pourrait être limité à un seul accès à la page d'inscription	• étape 3 : la remise d'un second justificatif d'identité par un autre mode (pas le courrier, c.-à-d. SMS) ajoute un élément dissuasif à l'usurpation d'identité • pourrait limiter pour chaque utilisateur (ID d'électeur) à un seul accès à la page d'inscription • l'ajout du PC à ce processus ajoute les mêmes inconvénients que dans le processus initial et contraint à un traitement additionnel des exceptions, ce qu'il sera très difficile de faire compte tenu de l'échéancier plus court

APPENDICE F : COMPARAISON DU REGISTRE DU SCRUTIN

	1	2
	Vote en réseau avec le registre du scrutin électronique (RSé)	***Vote en réseau sans le registre du scrutin électronique (RSé)***
HYPOTHÈSES	Le registre du scrutin électronique est requis si le vote en réseau à distance et sur site est mis en œuvre.	Le registre du scrutin électronique n'est pas requis si seul le vote en réseau à distance est mis en œuvre.
FLUX	**Flux du vote sur site** 1 Le votant présente l'ID au bureau de scrutin. 2 Dans le cas d'un vote sur papier, le membre du personnel de scrutin radie le votant par voie électronique au moyen du RSé. 3 Dans le cas d'un vote par ordinateur, le membre du personnel de scrutin utilise le registre du scrutin pour encoder un jeton avec l'ID/le mot de passe qui est archivé dans le système de vote. 4 Le votant insère la carte dans l'ordinateur, qui lit l'ID d'électeur et le mot de passe. 5 Le votant choisit les options de vote et dépose un bulletin de vote. 6 Le SVR traite le vote, et radie le votant par voie électronique. **Flux du vote à distance** 1 Le votant s'authentifie en ligne au moyen de l'ID d'électeur et du mot de passe. 2 Le système de vote en réseau traite le vote et radie le votant. 3 Le votant ne peut pas voter une deuxième fois en utilisant le mode à distance. 4 Le RSÉ est mis à jour en temps réel. 5 Si le votant se présente à un bureau de scrutin, le membre du personnel de scrutin verra que le votant a déjà voté.	**Flux du vote sur site** 1 La liste imprimée est distribuée aux bureaux de scrutin et indique les votants qui se sont inscrits pour voter à distance. 2 Le votant présente l'ID au bureau de scrutin et le membre du personnel de scrutin vérifie l'admissibilité sur la liste imprimée. 3 Le membre du personnel de scrutin donne un bulletin de vote uniquement aux votants qui ne sont pas inscrits pour voter en ligne. 4 Le membre du personnel de scrutin radie le votant de la liste des personnes qui votent sur papier. **Flux du vote à distance** 1 le votant s'inscrit pour voter à distance (au moyen d'un téléphone ou d'un ordinateur) avant le début de la période de vote par anticipation. 2 le votant s'authentifie en ligne au moyen de l'ID d'électeur et du mot de passe. 3 le système de vote en réseau traite le vote et radie le votant. 4 le votant ne peut pas voter une deuxième fois en utilisant le mode à distance. **Flux des révisions** 1 le personnel d'ÉO corrige et actualise la liste des votants à l'aide des systèmes et processus actuels finals. 2 les mises à jour sont synchronisées au besoin avec le

	1	2
	Vote en réseau avec le registre du scrutin électronique (RSé)	***Vote en réseau sans le registre du scrutin électronique (RSé)***
	Flux des révisions 1 Le personnel d'ÉO ajoute ou supprime des votants de la liste au moyen du RSÉ. 2 Les mises à jour sont synchronisées en temps réel avec le système de vote en réseau.	système de vote en réseau au moyen de processus manuels. 3 une synchronisation finale est effectuée entre le système de vote en réseau et le SGLE/SGE après l'événement.
DESCRIPTION	Un registre du scrutin électronique est requis dans un scénario qui combine le vote à distance avec mot de passe et le vote sur site par ordinateur au moyen d'une id physique. Comme le votant sur site prouve son identité à un membre du personnel de scrutin à l'aide d'un mécanisme physique, un mécanisme électronique est nécessaire pour relier la personne à l'identité (id d'électeur) archivée dans le système de vote en réseau. Ainsi, c'est le système qui détermine l'admissibilité (que le votant figure dans la liste et n'a pas voté auparavant).	Dans un scénario qui utilise seulement le vote en réseau à distance combiné aux bulletins de vote sur papier, un registre du scrutin en ligne n'est pas nécessaire à proprement parler, pourvu qu'un autre mode puisse être mis en œuvre pour empêcher les votants de voter en ligne, puis de voter sur un bulletin sur papier, ou l'inverse. Chaque mode (réseau et papier) gérera effectivement sa propre liste en parallèle et les besoins de synchronisation seront pris en charge manuellement à titre d'exceptions et ne seront pas traités en temps réel. - Le SGLE ou le SGE fournira la liste des électeurs finale versée au dossier et produira les listes sur papier qui sont utilisées dans les bureaux de scrutin.

1	2
Vote en réseau avec le registre du scrutin électronique (RSé)	***Vote en réseau sans le registre du scrutin électronique (RSé)***
Le registre du scrutin électronique est un système qui : établit un lien entre la personne sur site et l'identité inscrite dans le SVR s'intègre à la liste des électeurs finale (SGE) (y compris les révisions) et au système en ligne radie en temps réel (tous les modes simultanément, dont les bulletins de vote sur papier). Il est à noter que le système de vote en réseau tient également une liste électorale électronique qui est la liste des votants autorisés à voter au moyen des modes de scrutin en réseau. Peut fonctionner indépendamment de la liste des votants d'ÉO et est conçue pour fournir : a) la radiation en temps réel des votants en réseau; et b) l'établissement d'un lien entre les votants et les bulletins de vote chiffrés. n'est **pas facultative**, et devrait être comprise dans le produit de vote en réseau.	- Le SGLE ou le SGE fournira également au système de vote en réseau la liste des votants préliminaire (LVP). Le système de vote en réseau attribuera alors un identificateur unique à chaque électeur (l'ID d'électeur). Les électeurs qui désirent voter à distance s'inscriront en ligne ou par téléphone et associeront d'autres justificatifs d'identité à leur id d'électeur. L'inscription du votant doit prendre fin avant la date du scrutin par anticipation afin qu'il soit possible de générer et de distribuer les listes imprimées. Les électeurs qui s'inscrivent aux modes de scrutin en réseau à distance seront alors cantonnés au vote en réseau et ne pourraient voter sur un bulletin sur papier. (**des exceptions sont possibles pour les électeurs désireux de demander l'annulation de leurs justificatifs d'identité de VR pour qu'ils puissent voter sur papier*). La liste des votants se trouvant dans des bureaux de scrutin ne sera pas synchronisée automatiquement avec la liste de vote en réseau en ligne. La liste électorale électronique du système de vote en réseau renferme la liste des votants en temps réel qui sont autorisés à voter au moyen des modes de scrutin en réseau. Elle fonctionne indépendamment de la liste des votants d'ÉO et est conçue de manière à offrir a) la radiation en temps réel des personnes qui votent en réseau; et b) le lien des votants avec les bulletins de vote chiffrés. Elle n'est **pas facultative**, et sera comprise dans le produit de vote en réseau.

	1	2
	Vote en réseau avec le registre du scrutin électronique (RSé)	***Vote en réseau sans le registre du scrutin électronique (RSé)***
AVANTAGES	Appuie le principe d'un vote par votant en empêchant les votes multiples. Permet le vote sur site au moyen d'une identification physique (soit l'option la plus simple pour les votants). Permet la synchronisation en temps réel de la liste des votants (SGLE/SGE) avec Le système de vote en réseau (façon facile de traiter la mise à jour de la liste des votants).	Appuie le principe d'un vote par votant en empêchant les votes multiples (un sur papier, un à distance par ordinateur ou par téléphone). N'exige pas d'ordinateurs et de matériel sur site, ce qui réduit le coût et la complexité.
INCONVÉN-IENTS	Ajoute des coûts et de la complexité au scrutin - nécessite des ordinateurs et du matériel sur site - formation requise pour le personnel du scrutin. Ajoute des coûts à l'implantation par le fournisseur, selon : - l'ampleur de l'intégration avec les systèmes existants d'ÉO (SGLE/SGE) - les options de technologie à des fins d'intégration (services web, téléchargement de fichier).	Sans RSÉ, le système de vote en réseau en ligne ne sera pas synchronisé avec la liste dorsale des électeurs (SGLE/SGE). La mise à jour de la liste des votants doit donc être faite autrement : - A) gel de la liste de vote en réseau sur la base de la liste préliminaire des votants (LPV). Il s'agit d'une mesure raisonnable à prendre en situation de projet pilote, car le volume de révisions sera vraisemblablement bas (<5 % du total des noms). ou - B) mise à jour de la liste de VR (suppressions, changements aux ce) à la main, au fur et à mesure des révisions (p. ex. En utilisant une interface administrative du SVR ou en téléchargeant des fichiers de données).
RISQUES	L'intégration aux processus et systèmes d'ÉO pourrait ajouter de la complexité aux étapes d'adaptation et d'intégration du projet – y compris les aspects opérationnels dans les bureaux de vote.	Si les votants ne sont pas cantonnés, il y a de fortes chances qu'ils puissent voter deux fois (une fois à distance, une fois sur site). Bien que ce risque existe à l'heure actuelle dans le cas des scrutins par anticipation avec bulletins de vote sur papier, le risque aura encore plus d'ampleur dans le public dans le cas du vote en

	1 ***Vote en réseau avec le registre du scrutin électronique (RSé)***	2 ***Vote en réseau sans le registre du scrutin électronique (RSé)***
		réseau et devrait être géré différemment. Les votants devraient s'inscrire au vote en réseau, puis décider de ne pas voter de cette façon ou être empêchés de le faire. S'ils demeurent cantonnés, ils pourraient être complètement incapables de voter.
EXCEPTIONS	Ajouts et suppressions à la liste des votants sont traités en temps réel.	Pour gérer le risque, les électeurs inscrits au vote en réseau mais qui ne l'ont pas fait pourraient être « libérés » une fois la période de vote en réseau terminée pour pouvoir quand même voter sur papier le jour de scrutin. Ajouts à la liste de VR interdits une fois produite la liste de VR en ligne. Les votants qui doivent être supprimés de la liste en ligne une fois qu'ils sont dans le système de VR peuvent être retirés manuellement à l'aide d'une interface administrative.
SOLUTIONS DE RECHANGE	La fonctionnalité en ligne requise pourrait résider dans les systèmes d'ÉO, la solution du fournisseur, ou dans un système hybride. Cette décision serait prise en fonction : - de la capacité d'intégration et d'adaptation du fournisseur - de la capacité d'intégration et d'adaptation d'ÉO. Une intégration SVR/SGE plus simple est possible si aucune mise à jour en temps réel pour les nouveaux votants n'est requise : - L'intégration peut être aussi simple qu'une importation de fichiers qui aurait lieu avant le début du vote; une fois par jour en même temps que les mises à jour.	S'il est inacceptable de cantonner les votants dans le mode de vote en réseau, la liste du SGLE/SGE pourrait être synchronisée régulièrement (quotidiennement) avec le système de VR en ligne en examinant la liste des radiations sur papier et par voie électronique à partir de la liste de vote en réseau. Les votes en réseau déposés par les votants qui ont également voté en personne sur papier pourraient être retirés aussi souvent que quotidiennement, ou après l'élection. Bien que cette approche étaye le principe d'un vote par votant, elle laissera l'impression que le vote multiple est possible et présentera l'*apparence* que le

1	2
Vote en réseau avec le registre du scrutin électronique (RSé)	***Vote en réseau sans le registre du scrutin électronique (RSé)***
	principe n'est pas étayé.

APPENDICE G : DÉFINITIONS DES PRINCIPES

La liste de principes qui suit a été utilisée comme fondement du processus décrit dans le chapitre, qui précède (principes : évaluation du vote en réseau). C'est de cette liste complète qu'est tirée la liste finale des principes de base sur le vote en réseau. La liste est subdivisée en deux groupes : principes universels et principes procéduraux.

PRINCIPES UNIVERSELS

PRINCIPE DE BASE	PRINCIPE DÉTAILLÉ	DESCRIPTION
1. Universalité	1.1. Facilité d'emploi	Le processus de vote est facile à comprendre et à exécuter par les votants. Les votants ne doivent pas avoir besoin de compétences techniques, culturelles ou législatives particulières pour exprimer un suffrage.
	1.2. Accessibilité	Le processus de vote est également accessible à tous les votants admissibles, dont les votants handicapés. quoi qu'il en soit, le votant doit exécuter le processus de vote sans avoir besoin d'aide pour effectuer ses sélections.
	1.3. Facilité d'atteinte (emplacement)	Les moyens requis pour voter sont facilement réalisables par tout votant, indépendamment de l'emplacement du votant pendant la période de vote.
2. Égalité	2.1. Un votant, un vote	Un seul vote par votant est dénombré dans l'obtention des résultats de l'élection. Cette règle doit être suivie même si le votant a le droit de déposer des votes multiples.
	2.2. Pas de votants privilégiés	Aucun votant (individuel ou groupe) ne doit posséder un avantage technique, logique ou décisionnel sur les autres votants. Chaque vote a la même valeur, peu importe le votant qui le dépose.
	2.3. Pas d'acteurs privilégiés	Aucune personne ni entité impliquée dans la gestion ou l'application du processus électoral ne doit pouvoir influer sur le processus électoral ni recueillir de l'information qui n'est pas publique.

PRINCIPE DE BASE	PRINCIPE DÉTAILLÉ	DESCRIPTION
	2.4. Authentification et autorisation du votant	Le processus électoral doit s'assurer, avant de permettre à un votant de déposer un vote, que l'identité du votant est bien l'identité prétendue, que l'électeur est admissible à voter, et que les intentions de vote permises n'ont pas été excédées.
	2.5. Droit de figurer sur la liste des votants	Le processus électoral doit s'assurer que tous les votants admissibles sont inclus dans la liste des votants et que tous les votants peuvent faire valoir leur droit de vote s'ils n'y figurent pas.
	2.6. Compter seulement les votes des votants admissibles	Le processus électoral doit veiller à ce que les votes dépouillés dans le cadre du processus de dépouillement ont été déposés par des votants admissibles à voter.
	2.7. Organisation juste du bulletin de vote	Le processus de vote doit veiller à ce que toutes les options de vote, les parties et les candidats possèdent le même droit de figurer sur le bulletin de vote. La conception du bulletin de vote ou la distribution des options de vote ne doit favoriser aucun parti ni candidat. Ce principe devrait être préservé indépendamment du mode de scrutin utilisé par le votant pour déposer le vote.
	2.8. Absence de coût pour les votants	Les votants ne doivent pas engager de coûts précis liés à l'exercice de leur droit de vote.
	2.9. Production d'une liste des votants juste	Le processus électoral doit utiliser une liste des votants produite honnêtement qui se fonde uniquement sur des données de votants admissibles. tous les votants admissibles doivent être inclus dans la liste des votants.
3. Liberté	3.1. Ni contrainte ni vente de votes	Le processus de vote doit empêcher la contrainte et la vente de vote, généralement en ne fournissant pas au votant ou à un autre tiers de l'information qui pourrait être utilisée par la personne qui contraint ou par l'acheteur de votes pour deviner comment le votant entend voter.

PRINCIPE DE BASE	PRINCIPE DÉTAILLÉ	DESCRIPTION
	3.2. Vérifiabilité au cas par cas	Le processus de vote doit donner aux votants des moyens de vérifier que leurs votes ont été bien déposés dans l'urne (vote enregistré tel que déposé).
	3.3. Intégrité	Le processus de vote doit veiller à ce que l'issue de l'élection représente l'opinion des votants participants et qu'elle soit par conséquent obtenue seulement à partir des votes déposés par des votants admissibles. de plus, le processus de vote doit veiller à ce que les votes des votants admissibles n'ont pas été manipulés ou à ce qu'il n'y ait pas eu de remplissage d'urne.
4. Secret	4.1. Confidentialité des données personnelles	L'information liée aux votants doit être utilisée seulement aux fins spécifiques de l'élection et aucun acteur non autorisé ne peut y avoir accès.
	4.2. Secret du bulletin de vote	Le processus de vote doit préserver le secret des bulletins de vote déposés jusqu'à ce qu'ils doivent être traités dans le cadre du processus de dépouillement.
	4.3. Confidentialité	Le processus de vote doit empêcher à tous les stades de l'élection que l'on puisse établir une corrélation entre les votants et le contenu des bulletins de vote déposés par ces votants.
	4.4. Pas de résultats intermédiaires	Le processus de vote doit empêcher tout accès au contenu des votes déposés jusqu'au processus de dépouillement.
	4.5. Déclassement des données protégées	Le processus de vote doit comporter des pratiques de déclassement sécurisées du matériel, des dossiers et des données de vote qui pourraient mettre en péril la confidentialité des votants.

PRINCIPES PROCÉDURAUX

PRINCIPE DE BASE	PRINCIPE DÉTAILLÉ	DESCRIPTION
5. Transparence	5.1. Formation du votant	Le processus électoral devrait procurer des moyens d'apprendre et de comprendre le processus de vote avant l'élection.
	5.2. Information/diffusion	Le public devrait avoir accès à de l'information liée au processus électoral (calendrier, technologie, procédures, résultats de vérification, etc.). L'information doit être exacte et disponible assez longtemps avant l'élection.
	5.3. Facile à expliquer / comprendre par les votants	Le processus électoral doit être aussi simple et facile à comprendre que possible.
6. Vérifiabilité et responsabilisation	6.1. Vérifiabilité du code source	Le code source et les codes binaires de tout logiciel utilisé pour gérer les processus ou les données de l'élection doivent être disponibles à des fins de vérification et, au besoin, de certification. Le processus de vérification doit être mené à bien par des vérificateurs indépendants afin que le processus électoral se déroule bien.
	6.2. Vérifiabilité du processus	Le comportement des procédures suivies pendant le processus de l'élection doit être bien documenté et vérifiable afin que l'on puisse s'assurer qu'elles sont conformes aux exigences prévues.
	6.3. Certification	Le processus de vote et toute logique des composantes physiques qui y sont liées doivent être conçus pour faciliter la certification des éléments principaux de leur conception. La certification confirmera que le processus électoral de vote en réseau peut accomplir ce qui est établi dans les spécifications.
	6.4. Validation des résultats	le processus de vote doit offrir des façons de vérifier si les résultats représentent clairement l'intention des votants qui ont participé au processus de vote. Cette vérification doit également assurer que seuls les votes des votants admissibles ont été utilisés dans le processus de dépouillement pour empêcher les pratiques frauduleuses qui pourraient mettre en péril l'exactitude de l'élection.

PRINCIPE DE BASE	PRINCIPE DÉTAILLÉ	DESCRIPTION
	6.5. Surveillance de l'élection	Le processus de l'élection doit soutenir la surveillance de l'élection pour toutes les transactions effectuées au cours du processus. Ce processus de surveillance doit être solide et garantir que le secret du votant est préservé en tout temps.
	6.6. Examen des fichiers journaux/investigation informatique	Le processus de l'élection doit laisser des traces des activités exercées au cours du processus (p. ex. des fichiers journaux). Ces traces doivent être disponibles pour analyse pendant et après l'élection afin que l'on puisse s'assurer que le processus électoral se déroule bien.
	6.7. Reprises partielles possibles	Le processus de l'élection doit permettre la reprise d'une élection active à partir du même stade auquel elle a été stoppée sans perte de l'information qui était déjà enregistrée.
7. Fiabilité et sécurité	7.1. Disponibilité du service	Le processus de l'élection et toutes ses composantes ou entités essentielles (p. ex., information sur la liste électorale, votes déposés, mode de scrutin, etc.) doivent être à la disposition des votants, des gestionnaires de l'élection, des observateurs ou de tout autre acteur impliqué dans le processus pendant toute la période électorale.
	7.2. Pas de point de confiance commun	Le processus de l'élection ne doit accorder sa confiance à aucune entité unique (personne ou système) pour la mise en œuvre d'une étape essentielle. Les privilèges de l'entité doivent être limités par les politiques sur la répartition des tâches, afin d'exiger la collaboration de plusieurs entités de mise en œuvre des processus essentiels.
	7.3. Intégrité de la plateforme	Le processus de l'élection doit fournir des moyens de protéger l'intégrité et l'authenticité des entités et des composantes qui prennent part au processus. Ces moyens doivent être vérifiables au cours du processus de l'élection, afin de s'assurer de leur fonctionnement correct. Les procédures de vérification peuvent être exécutées avant et après le processus de l'élection.
	7.4. Contrôle d'accès	Le processus de l'élection doit fournir des moyens de contrôler et d'enregistrer l'accès des entités aux différentes étapes et composantes utilisées dans le cadre du processus.

PRINCIPE DE BASE	PRINCIPE DÉTAILLÉ	DESCRIPTION
	7.5. Intégrité de l'urne	Le processus de l'élection doit fournir des moyens de préserver et de détecter toute manipulation de l'urne.
	7.6. Intégrité des fichiers journaux	Le processus de l'élection doit fournir des moyens de préserver et de détecter toute manipulation des fichiers journaux ou registres des activités enregistrées pendant le processus.
	7.7. Intégrité de la liste des votants	Le processus de l'élection doit fournir des moyens de préserver et de détecter toute manipulation des données de la liste électorale.
	7.8. Intégrité de la configuration de l'élection	Le processus de l'élection doit fournir des moyens de préserver et de détecter toute manipulation des données de configuration de l'élection utilisées pour organiser l'élection.
	7.9. Intégrité des bulletins de vote	Le processus de l'élection doit fournir des moyens de préserver et de détecter toute manipulation des bulletins de vote déposés par un votant admissible.

GLOSSAIRE

A	**Attaque de type intermédiaire**	Forme d'interception illicite active dans laquelle le pirate établit des connexions indépendantes avec les victimes et retransmet les messages entre elles, en leur laissant croire qu'elles se parlent directement par connexion privée, alors que dans les faits, toute la conversation est contrôlée par le pirate. Le pirate doit être en mesure d'intercepter tous les messages entre les victimes et d'en transmettre de nouveaux. Une attaque de type intermédiaire peut réussir seulement lorsque le pirate peut usurper l'identité d'un point d'extrémité à la satisfaction de l'autre.
	Attaque entraînant un refus de service (RDS)	Tentative de rendre une ressource informatique (comme un site web) indisponible à ses utilisateurs prévus. Une méthode d'attaque fréquente consiste à saturer l'appareil ciblé de demandes. Ainsi, il ne peut prendre en charge le trafic légitime, ou il répond si lentement qu'il devient, dans les faits, indisponible.
	Authentification unique	Mécanisme qui permet aux utilisateurs d'accéder à un système après avoir été authentifiés dans un autre.
	Autorisation du votant	Mécanisme utilisé par un système de vote en réseau pour donner accès au système à un votant, afin qu'il puisse déposer un bulletin de vote. En général, l'autorisation suit l'identification du votant, quoique dans le cas du vote en réseau, le même mécanisme puisse assurer l'identification et l'autorisation du votant.
C	**Centre de données**	Infrastructure technique utilisée pour héberger les serveurs, généralement branchée à internet. Il existe plusieurs catégories de centres de données basées sur les niveaux de sécurité, de disponibilité et de rendement qu'ils offrent. Un système de vote en réseau exigera que les serveurs soient hébergés dans un centre de données fiable.
	Code d'utilisateur	Code constitué d'une série de caractères, généralement faciles à retenir et (ou) liés à des données relatives au votant, qui est utilisé pour identifier le votant dans un système de vote en réseau. S'accompagne habituellement d'un mot de passe pour authentifier le votant.
	Conseil de gestion du vote en réseau	Groupe de personnes chargées de superviser le traitement (le dépouillement) des bulletins de vote électroniques.

E	**Électeur**	Dans le contexte du présent document, le mot « électeur » désigne un ontarien qui a le droit de voter, qu'il interagisse ou non dans les faits avec un système ou un processus de vote. voir le terme « votant » pour établir la distinction entre les deux termes.
	Entité responsable de l'élection	Entité chargée de planifier, d'organiser et d'exécuter un processus électoral dans un territoire donné. dans le contexte du présent document, désigne élections Ontario.
	Étude de cas sur le vote en réseau :	Il s'agit du document qui présente les travaux de recherche effectués par Élections Ontario à propos du vote en réseau comme technologie permettant de voter d'autres façons. Il évalue la faisabilité d'un projet
I	**Identification du votant**	Mécanisme utilisé pour valider la déclaration d'un votant selon laquelle il est la personne qu'il prétend être. Il arrive que ce même mécanisme soit utilisé pour identifier et autoriser un votant, mais ce n'est pas toujours le cas.
J	**Justificatif d'identité de vote**	Les justificatifs d'identité de vote sont les éléments d'information utilisés par un électeur pour l'authentifier au moment du scrutin.
M	**Membre du personnel de scrutin**	Membres du personnel qui travaillent dans un bureau de scrutin au cours du processus électoral et qui sont chargés d'identifier les votants et de faciliter le processus électoral.
	Mot de passe	Combinaison de caractères, généralement alphanumériques, que seul le votant connaît et qui est utilisée par le système de vote pour authentifier les votants. Habituellement, les mots de passe s'accompagnent d'un « code d'utilisateur » unique (un par votant). Il arrive que le code d'utilisateur et le mot de passe puissent être combinés en une série unique de caractères appelée NIV.
	Mystification	Reproduction d'une page web légitime sur un serveur contrôlé par un pirate dans le but de tromper les utilisateurs en les amenant à penser qu'ils sont branchés à un site de confiance.
N	**NIP**	Il s'agit du numéro d'identification personnel, généralement utilisé par les votants pour avoir accès à un téléphone mobile ou à une carte à puce intelligente. Il est à noter que le NIP est différent du NIV.

	NIV	Désigne le numéro d'identification du votant, qui est constitué d'une combinaison de caractères pouvant être utilisés pour authentifier un votant. Un NIV est généralement utilisé pour remplacer le couple code d'utilisateur/mot de passe.
P	**Passerelle SMS**	Infrastructure technique utilisée pour envoyer et recevoir de courts messages texte en grande quantité. règle générale, ce sont des sociétés spécialisées qui offrent ce service et qui peuvent exploiter les divers réseaux cellulaires.
	Processus d'authentification	Processus de confirmation de l'identité du votant et d'autorisation de l'accès au système de vote.
R	**Reniflage de réseau**	Également connu sous le nom d'« analyseur de paquet », le renifleur de réseau est un programme qui intercepte et enregistre le trafic sur un réseau pour tenter d'analyser l'activité qui s'y déroule. Un renifleur peut comporter de nombreuses utilisations légitimes, dont la détection des intrusions et la surveillance de système, ou pourrait être utilisé pour espionner les utilisateurs et recueillir de l'information délicate.
	RTCP	Réseau téléphonique commuté public
	RVI – Réponse vocale interactive	Système offrant une interface sonore aux votants pour qu'ils puissent déposer des bulletins de vote au moyen d'un téléphone conventionnel.
S	**Sécurité de bout en bout (chiffrement)**	Façon de s'assurer que les bulletins de vote déposés par les votants sont protégés depuis leur origine, afin que seuls les responsables de l'élection puissent traiter les bulletins de vote (c'est-à-dire qu'aucun pirate externe ni technicien interne du système de vote ne peut affecter l'intégrité des bulletins de vote ou la vie privée du votant).
	Technologie permettant de voter d'autres façons :	Inclut deux volets technologiques pour le vote. Ces volets sont les suivants : Les technologies permettant de voter d'autres façons non reliées à un réseau (voir technologie d'aide au vote), et Les technologies permettant de voter d'autres façons reliées à un réseau (voir vote en réseau).

	Technologie d'aide au vote :	L'un des deux volets de la technologie permettant de voter d'autres façons. C'est le nom qu'Élections Ontario donne à l'équipement de vote disponible sur le lieu de vote sans être relié à un réseau, et qu'il est obligatoire de mettre à la disposition des électeurs, comme indiqué dans l'article 44.1 de la loi électorale.
V	**VOIP**	Protocole de voix sur ip, soit un protocole de communications permettant la transmission de la communication par la voix sur internet.
	Votant	Dans le contexte du présent document, le mot « votant » désigne une personne qui interagit avec un système ou un processus de vote et qui exerce donc activement son droit à titre d'électeur. Un « électeur » devient un « votant » lorsqu'il accepte un bulletin de vote dans un lieu de vote ou s'authentifie à l'aide du système de vote en réseau. voir « électeur » pour établir la distinction entre les deux termes.
	Vote électronique	Le vote électronique (ou cybervote) est un terme qui englobe plusieurs types de vote différents. Il comprend les méthodes électroniques de dépôt et de dépouillement de votes. La technologie de vote électronique peut comprendre les cartes perforées, les systèmes de vote à lecteur optique et les bornes interactives de vote spécialisées (dont les systèmes de vote électroniques autonomes à enregistrement direct, ou SEED). Cette technologie peut en outre englober la transmission de bulletins de vote et de votes par téléphone, par réseaux informatiques privés, ou par internet.
	Vote électronique à distance	Il s'agit du terme privilégié pour désigner le vote par un moyen électronique à partir de n'importe quel emplacement, sans supervision directe de la part des responsables de l'élection. Ces moyens électroniques pourraient comprendre l'utilisation d'internet, d'un message texte, de la télévision numérique interactive, ou encore d'un appareil téléphonique à clavier.
	Vote électronique sur site	Terme utilisé pour définir le processus de vote qui a lieu dans des endroits supervisés (p. ex. des bureaux de vote) au moyen d'appareils électroniques. Ces appareils peuvent être isolés ou branchés à un réseau.
	Vote en réseau	Tout type de vote par voie électronique qui comporte le dépôt et l'envoi des bulletins de vote sous forme électronique à une installation centrale.

Vote par internet	Le vote par internet est une mise en œuvre spécifique du vote électronique à distance, par lequel le vote a lieu sur internet, notamment sur un site web. Le terme est parfois utilisé de manière interchangeable avec le terme « vote électronique à distance ». Cet usage est désuet et le terme « vote par internet » ne désigne maintenant qu'un sous-ensemble précis du vote électronique à distance.
Vote par téléphone	Cas précis de vote en réseau, dans le cadre duquel le vote est déposé au moyen d'un téléphone. L'interface du votant est basée sur la voix, sur un système de menu et sur la saisie de données numériques.

---

[1] *http://www.e-laws.gov.on.ca/html/statutes/french/elaws_statutes_90e06_f.htm*

[2] *http://www.elections.on.ca/fr-CA/AboutUs/Mission.htm?lang=fr*

[3] *http://www.Ontario.ca/fr/login/ONT03_026064.html*

[4] *http://www.e-laws.gov.on.ca/html/statutes/french/elaws_statutes_90e06_f.htm*

[5] Élections Canada: Sondage auprès des électeurs à la suite de la 40e élection générale, Sondage postélection de 2007 d'Ipsos Reid

[6] *http://www.statcan.gc.ca/daily-quotidien/100510/t100510a1-fra.htm*

[7] *http://www40.statcan.gc.ca/l01/cst01/comm32a-fra.htm*

[8] *http://www40.statcan.gc.ca/l01/cst01/comm29a-fra.htm*

[9] *http://www.statcan.gc.ca/daily-quotidien/100510/dq100510a-fra.htm*

[10] *http://www.statcan.gc.ca/daily-quotidien/070504/dq070504a-fra.htm*

[11] *http://webaim.org/blog/screen-reader-user-survey-3-results/*

[12] Statistique fournie au Sommet d'apprentissage sur le vote électronique aux élections municipales, Toronto, 15 décembre 2010

[13] Peterborough, 2010 : 16 % des votes déposés l'avaient été en réseau

[14] *Les principes utilisés comme base de cette analyse reposaient sur ceux qui étaient recommandés par le Conseil de l'Europe. http://www.coe.int/t/dgap/democracy/activities/ggis/E-voting/Key_Documents/Rec(2004)11_Eng_Evoting_and_Expl_Memo_fr.pdf*

[15] Par exemple, le permis de conduire plus de l'Ontario contient une puce d'identification par radiofréquence (IRF) qui archive seulement un numéro d'identification unique indiquant la citoyenneté canadienne. Il est conçu comme solution de rechange au passeport à la frontière Canada-États-Unis.

[16] Le service ONe-key lancé par ServiceOntario constituera vraisemblablement un très bon candidat pour cette approche.

17 Ces mesures de contrôle sont liées à la section sur les exigences du système de vote en réseau (voir Appendice A : Exigences détaillées).

[18] L'information doit comprendre au moins le nombre de votants, afin que des justificatifs d'identité puissent être produits, autrement dit, le SVR n'aurait pas besoin des vrais noms si le SGE les couvre.

[19] *Le projet de règlement sur les Normes d'accessibilité intégrées a été affiché pour examen public du 1er février au 18 mars 2011. L'article 14 de la partie II traite de l'accessibilité des sites Web.*