Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF

Section des droits politiques

1er mars 2023

Appréciation des risques Vote électronique de la Chancellerie fédérale 2023

Résumé exécutif

Avec la restructuration de la phase d'essai, il a été décidé que chacun des acteurs devait maintenant conduire une appréciation des risques couvrant ses responsabilités dans le cadre du vote électronique (mesure B.5 du catalogue de mesures du rapport final du Comité de pilotage Vote électronique du 30 novembre 2020 concernant la restructuration et la reprise des essais[1]). Cette appréciation des risques vise à maintenir les risques à un niveau acceptable et sert à l'évaluation des demandes d'agrément déposées par les cantons en vue de l'utilisation d'un système de vote électronique dans le cadre d'un scrutin fédéral. Par souci de transparence, la Chancellerie fédérale (ChF) a décidé de publier son appréciation des risques ainsi que le processus qui la régit.[2]

Les risques de l'utilisation du vote électronique dans des décisions politiques, en l'absence de toute mesure de protection, sont élevés. C'est pourquoi la ChF a tout d'abord évalué la situation en l'absence de mesures, afin d'identifier les risques prioritaires, puis appliqué les mesures actuellement en vigueur, qu'elles soient de nature légale, financière, sociale, scientifique ou organisationnelle, afin d'avoir la vue courante des risques. Dans cet exercice, elle a également considéré les connaissances actuelles en matière politique, administrative, sécuritaire et technique. Cette vue, représentée dans la carte des risques résiduels ci-dessous, montre que la grande majorité des risques sont actuellement évalués comme ayant un niveau suffisamment bas (zones vertes de la carte). Si l'évolution de l'ensemble des risques doit toujours être surveillée, il en subsiste quatre (R2, R11, R13 et R14) qui doivent faire l'objet d'une attention particulière selon les critères de traitement des risques définis dans le processus de gestion des risques Vote électronique de la ChF[2]. Les risques R3 et R5 relatifs respectivement à l'acceptation du vote électronique et à la disponibilité d'une plateforme anonyme d'achat de votes, bien qu'acceptables selon les critères de traitement, font également l'objet d'une attention particulière.

En sus des mesures déjà prises, la ChF et les cantons maintiennent un catalogue de mesures[2] futures qui pourront permettre de réduire encore les risques.

---

[1] www.bk.admin.ch > Droits politiques > Vote électronique > Rapports et études

[2] www.bk.admin.ch > Droits politiques > Vote électronique > Essais de vote électronique

Probabilité	Score d'impact: 32 – 49 (Haut)	Score d'impact: 22 – 31 (Moyen)	Score d'impact: 17 – 21 (Bas)
Haut			
Moyen			**R4** Campagne de dénigrement du vote électronique dans les médias (sociaux) **R5** Achat de votes sur une plateforme anonyme **R7** Violation du secret du vote par un état tiers **R8** Indisponibilité du système suite à une attaque par un état tiers
Bas	**R2** Défaut de détection des erreurs systématiques **R11** Mise en œuvre d'un système différent de celui autorisé **R13** Manque d'experts indépendant **R14** Nouvelles technologies menaçant le secret du vote	**R3** Manque d'acceptation du vote électronique **R6** Manipulation des votes par un état tiers **R9** Exigences inadéquates **R10** Autorisation d'un système défaillant **R15** Perte du système pendant un scrutin **R16** Suppression du canal vocal en raison d'une coopération défaillante **R17** Suppression du canal de vote en raison d'un manque de ressources **R18** Dépassement des plafonds légaux	**R1** Faille sévère dans le système **R12** Mise en danger du développement des exigences de sécurité

Tableau 1 : Carte des risques résiduels après la mise en œuvre des mesures de mitigation

Table des matières

1 Champs d'application et objectifs

Le présent document est établi et maintenu par la Chancellerie fédérale (ChF) en conformité avec la mesure B.5 du catalogue de mesures du rapport final du Comité de pilotage Vote électronique (CoPil VE) du 30 novembre 2020 concernant la restructuration et la reprise des essais de vote électronique[3]. Il est issu du processus de gestion des risques Vote électronique de la Chancellerie fédérale[4] et représente la perspective de la ChF sur ses propres risques en lien avec le vote électronique. Les appréciations des risques des cantons menant des essais de vote électronique sont prises en considération dans l'évaluation des risques de la ChF. Il se base sur le guide pour l'appréciation des risques de la ChF[5] en cela qu'il suit une méthodologie d'identification, d'analyse et d'évaluation des risques similaire ainsi qu'il traite d'une partie des risques administratifs et politiques qui y sont référencés, tel que cela est prévu par le guide de la ChF.

En sus de sa contribution aux objectifs définis dans le processus de gestion des risques Vote électronique de la Chancellerie fédérale, il sert également à l'évaluation des demandes d'agrément déposées par les cantons en vue de l'utilisation d'un système de vote électronique dans le cadre d'un scrutin fédéral.

2 Identification des risques

En se basant sur les actifs identifiés dans le processus de gestion des risques Vote électronique de la ChF, les risques suivants ont été identifiés. Certains risques proviennent du guide pour l'appréciation des risques de la ChF. La référence au guide est indiquée dans la colonne Référence dans ce cas.

Identifiant	Description	Actifs	Référence
ChF-VE-R1	Une faille de sécurité sévère affectant le système est découverte pendant le scrutin.	Résultats du scrutin fédéral Confiance des électeurs Scrutin fiable avec vote électronique	
ChF-VE-R2	Des signalements de codes de vérification erronés sont faits dans plusieurs cantons mais aucune alerte n'est lancée au niveau national faute de coordination entre les cantons et la ChF.	Résultats du scrutin fédéral Scrutin fiable avec vote électronique	RPA-10
ChF-VE-R3	Le vote électronique n'est pas suffisamment accepté.	Confiance des électeurs	
ChF-VE-R4	Une campagne de dénigrement du vote électronique est lancée sur les réseaux sociaux ou dans les médias. Celle-ci peut se baser sur des événements en lien avec le vote électronique à l'étranger, le supposé manque de contrôle public des processus de vote, de fausses allégations relatives aux mécanismes de la vérifiabilité ou une communication défaillante des autorités.	Confiance des électeurs	RPA-6
ChF-VE-R5	Une campagne d'achat de votes est lancée et propose une plateforme en ligne permettant aux électeurs de vendre leur vote électronique.	Confiance des électeurs Scrutin fiable avec vote électronique	RPA-9

[3] www.bk.admin.ch > Droits politiques > Vote électronique > Rapports et études

[4] www.bk.admin.ch > Droits politiques > Vote électronique > Essais de vote électronique

[5] www.bk.admin.ch > Droits politiques > Vote électronique > Exigences du droit fédéral

Identifiant	Description	Actifs	Référence
ChF-VE-R6	Un état tiers* mobilise ses services et réussi à manipuler les votes dans le système.	Résultats du scrutin fédéral Confiance des électeurs Scrutin fiable avec vote électronique	
ChF-VE-R7	Un état tiers* mobilise ses services et réussi à violer le secret du vote.	Confiance des électeurs Scrutin fiable avec vote électronique	
ChF-VE-R8	Un état tiers* mobilise ses services et réussi à influencer le résultat du scrutin en excluant des votants.	Résultats du scrutin fédéral Confiance des électeurs Scrutin fiable avec vote électronique	
ChF-VE-R9	Exigences inadéquates qui ne permettent plus de maintenir le niveau de sécurité voulu.	ODP et OVotE	
ChF-VE-R10	La Confédération a autorisé l'utilisation d'un système dont les mesures de sécurité ne satisfont pas les exigences légales.	Résultats du scrutin fédéral Confiance des électeurs Scrutin fiable avec vote électronique	RPA-2
ChF-VE-R11	Déploiement et utilisation d'un système différent de celui autorisé.	Résultats du scrutin fédéral Confiance des électeurs Scrutin fiable avec vote électronique	
ChF-VE-R12	Désintérêt des experts pour le vote électronique qui conduit à une stagnation puis une obsolescence des exigences de sécurité.	Experts indépendants et compétents	
ChF-VE-R13	Manque d'experts indépendants qualifiés pour la conduite des contrôles.	Experts indépendants et compétents	
ChF-VE-R14	Développement à large échelle d'une nouvelle technologie rendant obsolètes les exigences de sécurité en matière de protection du secret du vote (p. ex. ordinateur quantique).	Confiance des électeurs ODP et OVotE Scrutin fiable avec vote électronique	
ChF-VE-R15	Le fournisseur de système n'est plus en mesure de fournir son système pendant un scrutin alors que des votes ont déjà été émis.	Résultats du scrutin fédéral Fournisseurs de système Scrutin fiable avec vote électronique	
ChF-VE-R16	Des différends nuisent à la coopération entre les autorités entre elles et/ou les fournisseurs de systèmes, de sorte que le vote électronique ne peut plus être développé ou est interrompu.	Cantons participants aux essais Fournisseurs de système	RPA-3
ChF-VE-R17	Les cantons manquent de ressources pour la mise en œuvre du vote électronique.	Cantons participants aux essais	RPA-8

Identifiant	Description	Actifs	Référence
ChF-VE-R18	L'utilisation effective du canal de vote électronique dépasse les limites de l'électorat autorisé (30% cantonal et 10% national).	Confiance des électeurs Cantons participants aux essais Scrutin fiable avec vote électronique	

Tableau 2 : Catalogue des risques

* Les risques liés à des attaquants qui ne sont pas des états tiers ne sont pas inscrits dans la liste car il est admis que l'état tiers représente l'attaquant avec le plus de moyens et de connaissances. Les autres catégories d'attaquants ne nécessitent donc pas de mesures supplémentaires par rapport à celles prises pour contrer cet attaquant. Les moyens envisagés comme une attaque interne par le personnel du fournisseur de système ou du canton ou une attaque directe de la plateforme du votant sont couverts par ces risques.

3 Événements et connaissances pertinents pour l'analyse des risques

3.1 Politique et réglementation

3.1.1 Renoncement à une mise en exploitation ordinaire

Lors de sa séance du 26 juin 2019, le Conseil fédéral a décidé de renoncer à passer à la mise en exploitation ordinaire du vote électronique. Lors de la consultation portant sur le projet de modification de la loi fédérale sur les droits politiques, la majorité des participants se sont certes prononcés en faveur du vote électronique, mais la plupart des partis, en particulier, ont jugé prématuré le passage à sa mise en exploitation ordinaire.

3.1.2 Restructuration de la phase d'essai

Le Conseil fédéral a chargé la ChF, le 26 juin 2019, de concevoir avec les cantons une restructuration de la phase d'essai du vote électronique, l'objectif étant de mettre en place une phase d'essai stable reposant sur des systèmes de vote électronique offrant la vérifiabilité complète. La restructuration de la phase d'essai se fait en fonction des objectifs suivants :

- Poursuite du développement des systèmes
- Surveillance et contrôles efficaces
- Renforcement de la transparence et de la confiance
- Renforcement des liens avec les milieux scientifiques

La ChF et les cantons ont établi en commun un rapport final consacré à la restructuration et à la reprise des essais. Pour ce faire, ils ont mené un vaste dialogue avec des experts issus de la science et de l'industrie, après quoi ils ont rédigé le rapport final et l'ont assorti d'un catalogue de mesures. Celui-ci prévoit un échelonnement des mesures dans la perspective de la reprise des essais.

Le Conseil fédéral a pris acte du rapport final du CoPil VE lors de sa séance du 18 décembre 2020. Il a chargé la ChF de mettre en œuvre par étapes les mesures nécessaires à la restructuration des essais.

La première étape de la restructuration a été la révision des bases légales. Les projets de révision partielle de l'ordonnance sur les droits politiques (ODP ; RS 161.11) et de révision totale de l'ordonnance de la ChF sur le vote électronique (OVotE ; RS 161.116) sont entrées en vigueur le 1er juillet 2022. Ils permettent d'améliorer la sécurité des systèmes de vote électronique, d'abord, en prévoyant que seuls seront désormais autorisés les systèmes entièrement vérifiables et ayant été contrôlés par des experts indépendants sur mandat de la Confédération, ensuite, en précisant et en renforçant les exigences de sécurité et de qualité auxquelles ces mêmes systèmes, leur utilisation et leur développement doivent répondre. Ils ne pourront en outre être utilisés que pour 30 % au plus de l'électorat cantonal et 10 % de l'électorat suisse dans son ensemble.

Les nouvelles bases légales renforcent les exigences de transparence et prévoient la participation du public et des milieux spécialisés. Les conditions applicables à la publication d'informations sur le système

et son exploitation ont ainsi été précisées, et celles qui régissent la participation du public, comme l'obligation de mettre en place un programme permanent de bug bounty (versement d'une prime pour la découverte d'une faille), ont été ajoutées.

La collaboration avec les experts n'aura pas seulement lieu dans le cadre du contrôle indépendant des systèmes, mais sera institutionnalisée sous la forme d'un suivi permanent des essais de vote électronique. Le dialogue avec les milieux scientifiques, qui a déjà eu lieu pour la restructuration des essais, sera poursuivi et même inscrit formellement dans les textes. Il est prévu dans les années à venir de mettre en œuvre un important catalogue de mesures[6], qui permettra d'améliorer en continu les systèmes de vote électronique et leur exploitation.

3.2 Sécurité

3.2.1 Publication du code source et test public d'intrusion 2019

En février 2019, La Poste Suisse a publié le code source de son nouveau système comportant la vérifiabilité complète ainsi que la documentation qui l'accompagne. Ce système a en outre été soumis à un test public d'intrusion entre le 25 février et le 24 mars 2019. La publication du code source a permis de mettre en évidence deux failles majeures. Une troisième faille a par ailleurs été découverte, affectant la vérifiabilité individuelle et donc le système de la Poste déjà en service à ce moment. Suite à ces découvertes, la Poste a retiré ce système.

3.2.2 Contrôle indépendant 2021-2023

La ChF a lancé le 5 juillet 2021 le contrôle indépendant du système de vote électronique de la Poste avec vérifiabilité complète et de son exploitation. Le contrôle a été confié à des experts issus de la science et de l'industrie. Il s'est globalement terminé en janvier 2023. Il reste quelques corrections qui doivent être faites et vérifiées avant la reprise des essais. Ces dernières sont faciles à mettre en œuvre et à contrôler et présentent donc un risque faible.

Les derniers résultats montrent que le système de vote électronique de la Poste a été considérablement amélioré depuis 2019. Des manquements importants ont pu être identifiés et corrigés. Les rapports indiquent toutefois que des mesures supplémentaires doivent être prises. Dans l'optique d'une amélioration continue, la Confédération et les cantons se sont mis d'accord sur la mise en œuvre de ces mesures et les ont consignées dans le catalogue.

Les résultats du contrôle indépendant font partie des éléments dont le Conseil fédéral tient compte lorsqu'il décide d'accorder ou non une autorisation générale à un canton qui en fait la demande.

3.2.3 Publication du code source et de la documentation du système de la Poste et de son exploitation ainsi que programme de *bug bounty* depuis 2021

En application de l'art. 13 de l'OVotE révisée, la Poste a publié l'intégralité de son système de vote électronique avec vérifiabilité complète et ce de manière pérenne. Elle conduit également un programme continu de *bug bounty* (prime aux bogues) qui permet au public de fournir des indications qui touchent à la sécurité et qui permettent d'améliorer le système tout en étant rémunéré de manière équitable pour cela. Des spécialistes ont ainsi la possibilité d'analyser les documents et de tester le code source. L'objectif de ces mesures est d'identifier suffisamment tôt les éventuelles failles dans le système sur la base des signalements et de les éliminer.

En décembre 2022, la Poste indique que plus de 180 signalements ont été reçus depuis 2021, dont quatre avec un degré de gravité « élevé ». Au total, un peu plus de 120'000 euros ont été versés pour les signalements.[7]

---

[6] www.bk.admin.ch > Droits politiques > Vote électronique > Essais de vote électronique

[7] https://evoting-community.post.ch/fr

Un test d'intrusion public (PIT) a en outre eu lieu du 8 août au 2 septembre 2022. La Poste a documenté la participation d'environ 3'400 participants ainsi que la réception de deux signalements. L'un des signalements a été confirmé avec un degré de gravité « faible » et récompensé par une prime de 500 CHF. Aucune intrusion dans l'infrastructure ou dans l'urne électronique n'a eu lieu. La Poste a publié un rapport final sur le PIT.[8] Le programme de *bug bounty* se poursuit en conformité avec les exigences légales.

3.2.4 Environnement numérique de plus en plus hostile

Si les attaques contre les systèmes informatiques existent depuis bien longtemps, force est de constater qu'elles se sont intensifiées ces derniers mois/années.[9] Elles ne se cantonnent plus aux grandes entreprises mais s'étendent aux pouvoirs publics. Si l'appât du gain semble être la motivation principale, les motivations idéologiques ou politiques en ont également toujours fait partie. De plus, l'essor des plateformes de malware-as-a-service contribue à augmenter l'accessibilité des outils nécessaires pour mener une cyberattaque et diminue le niveau de compétence requis pour l'élaboration de cette dernière.[10] Finalement, un groupe de hackers exploitant une plateforme de rançongiciel as-a-service appelée LockBit conduit depuis juin 2022 la première campagne de *bug bounty* (prime aux bogues) pour logiciels malveillants et récompense ceux qui lui fournissent des indications sur des failles dans des systèmes qu'il pourrait potentiellement attaquer ou des améliorations de ses logiciels d'attaque.[11]

La cybercriminalité reste la menace la plus immédiate pour les infrastructures critiques. Elle peut être aussi bien motivée par l'appât du gain pour ce qui est des acteurs privés que par une volonté de déstabilisation du système en place pour ce qui est des acteurs étatiques. Juste avant et pendant la guerre menée par la Russie contre l'Ukraine, des cyberattaques ont été lancées contre les infrastructures critiques ukrainiennes. Si, pour des raisons politiques, la Suisse se retrouve dans la ligne de mire d'acteurs étatiques ou non disposant des capacités nécessaires, la probabilité d'une cyberattaque augmente. Selon le rapport de situation du Service de renseignement de la Confédération, bien qu'un sabotage spécifiquement dirigé vers la Suisse soit très improbable et que des faits d'hacktivisme contre la Suisse soient plutôt improbables, les attaques dans le domaine de la désinformation contre des institutions suisses sont plutôt probables. Le cyberespionnage contre la Suisse est quant à lui très probable.[10] La prise de mesures contre certains intérêts russes par la Suisse pourrait également avoir des conséquences en termes d'exposition aux cyberattaques pour la maintenance d'infrastructures critiques informatiques.[9]

La vérifiabilité telle que définie dans l'OVotE est conçue afin d'offrir un niveau de protection adéquat même contre un environnement particulièrement hostile. De plus, les infrastructures et logiciels liés au vote électronique font partie des infrastructures critiques[12] qui peuvent recevoir le soutien des services fédéraux concernés en cas d'attaque.

3.3 Technologie

3.3.1 Ordinateur quantique

Les ordinateurs quantiques pourraient poser un problème pour les mécanismes de chiffrement asymétriques (RSA, El Gamal, Diffie-Hellman) en particulier, car il existe déjà un algorithme quantique (algorithme de factorisation de Shor[13]) permettant de résoudre ces problèmes efficacement et donc de décrypter les données chiffrées par ces mécanismes. Cependant, bien que le domaine se développe rapidement et fasse l'objet de beaucoup d'investissements, il reste encore très loin d'une application con-

---

[8] https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master/Reports/PublicIntrusionTest

[9] www.ncsc.admin.ch > Documentation > Rapports > Rapports sur la situation

[10] Rapport de situation du Service de renseignement de la Confédération - la sécurité de la Suisse 2022

[11] https://www.bleepingcomputer.com/news/security/lockbit-30-introduces-the-first-ransomware-bug-bounty-program

[12] www.babs.admin.ch > Autres domaines d'activité > Protection des infrastructures critiques

[13] https://fr.wikipedia.org/wiki/Algorithme_de_Shor

crète. Les ordinateurs quantiques nécessitent un environnement très particulier pour fonctionner correctement et sont très sensibles aux perturbations.[14] IBM vise la fin 2023 pour le développement d'un processeur quantique avec 1'000 qubits[15, 16]. Il est actuellement admis qu'il faudrait un nombre de qubits deux fois plus grand que ce le nombre de bits servant à coder le nombre à deviner dans une mise en application de l'algorithme de Shor mentionné plus haut. Pour une clé RSA de 2048 bits, il faudrait donc un ordinateur quantique disposant de plus de 4000 qubits. Il est actuellement très difficile de prédire l'évolution de cette technologie.[17]

Le National Institute of Standards and Technology (NIST)[18] a lancé un processus de sélection et de standardisation de procédés cryptographiques post-quantiques en 2016[19]. Le 3e round de sélection s'est achevé en 2020 et les projets de normes devraient être disponibles d'ici à 2024.

En attendant l'avènement d'algorithmes standards post-quantiques, il est toujours possible de prévenir et de mitiger l'impact de l'évolution des ordinateurs quantiques sur les mécanismes de chiffrement actuels par l'augmentation de la taille des clés de chiffrement utilisées. Le système de la Poste utilise actuellement des clés de 3072 bits. De même, des procédés de chiffrement sûrs en théorie de l'information peuvent entraver la réussite de l'utilisation d'ordinateurs quantiques.

4 Analyse et évaluation des risques

De nombreuses mesures sont et seront prises pour mitiger les risques du vote électronique. Le tableau suivant présente de manière succincte l'évaluation des risques avant la prise de toute mesure de mitigation. L'évaluation détaillée est disponible en annexe. À noter que le score du risque se base sur les conséquences de la réalisation de ce dernier alors que la probabilité du risque se limite à l'événement mentionné dans sa description. La probabilité indiquée ici n'est donc pas liée au pire scénario envisagé dans l'annexe qui, en général, a une probabilité plus faible d'arriver qu'un scénario plus optimiste. L'évaluation après mitigation est présentée dans le chapitre sur les risques résiduels (voir ch. 6).

Identifiant	Description	Score	Probabilité
ChF-VE-R1	Une faille de sécurité sévère affectant le système est découverte pendant le scrutin.	40	Moyenne
ChF-VE-R2	Des signalements de codes de vérification erronés sont faits dans plusieurs cantons mais aucune alerte n'est lancée au niveau national faute de coordination entre les cantons et la ChF.	44	Moyenne
ChF-VE-R3	Le vote électronique n'est pas suffisamment accepté.	33	Moyenne
ChF-VE-R4	Une campagne de dénigrement du vote électronique est lancée sur les réseaux sociaux ou dans les médias. Celle-ci peut se baser sur des événements en lien avec le vote électronique à l'étranger, le supposé manque de contrôle public des processus de vote, de fausses allégations relatives aux mécanismes de la vérifiabilité ou une communication défaillante des autorités.	29	Haute
ChF-VE-R5	Une campagne d'achat de votes est lancée et propose une plateforme en ligne permettant aux électeurs de vendre leur vote électronique.	43	Moyenne
ChF-VE-R6	Un état tiers mobilise ses services et réussi à manipuler les votes dans le système.	43	Moyenne
ChF-VE-R7	Un état tiers mobilise ses services et réussi à violer le secret du vote.	38	Moyenne

[14] Present landscape of quantum computing – Hassija – 2020 – IET Quantum Communication – Wiley Online Library

[15] Les qubits sont une unité de mesure de la puissance des ordinateurs quantiques. Sommairement, plus un ordinateur quantique a de qubits plus grand sont les nombres qu'il peut manipuler. Cependant, tous les qubits ne peuvent être utilisés pour le calcul car, selon la technologie utilisée, une partie d'entre eux doit être dévolue à la correction d'erreur. Aussi IBM a introduit une nouvelle unité de mesure qui est le volume quantique et qui ne tient compte que des qubits effectivement utilisables de façon fiable.

[16] https://research.ibm.com/blog/ibm-quantum-roadmap

[17] Quantum Attack Resource Estimate: Using Shor's Algorithm to Break RSA vs DH/DSA VS ECC – Kudelski Security Research

[18] L'institut national des normes et de la technologie, est une agence du département du Commerce des États-Unis. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des normes de concert avec l'industrie.

[19] https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

Identifiant	Description	Score	Probabilité
ChF-VE-R8	Un état tiers mobilise ses services et réussit à influencer le résultat du scrutin en excluant des votants.	31	Moyenne
ChF-VE-R9	Exigences inadéquates qui ne permettent plus de maintenir le niveau de sécurité voulu.	40	Basse
ChF-VE-R10	La Confédération a autorisé l'utilisation d'un système dont les mesures de sécurité ne satisfont pas les exigences légales.	47	Moyenne
ChF-VE-R11	Déploiement et utilisation d'un système différent de celui autorisé.	44	Moyenne
ChF-VE-R12	Désintérêt des experts pour le vote électronique qui conduit à une stagnation puis une obsolescence des exigences de sécurité.	40	Moyenne
ChF-VE-R13	Manque d'experts indépendants qualifiés pour la conduite des contrôles.	32	Moyenne
ChF-VE-R14	Développement à large échelle d'une nouvelle technologie rendant obsolètes les exigences de sécurité en matière de protection du secret du vote (p. ex. ordinateur quantique).	35	Basse
ChF-VE-R15	Le fournisseur de système n'est plus en mesure de fournir son système pendant un scrutin alors que des votes ont déjà été émis.	40	Basse
ChF-VE-R16	Des différends nuisent à la coopération entre les autorités et les fournisseurs de systèmes, de sorte que le vote électronique ne peut plus être développé ou est interrompu.	23	Moyenne
ChF-VE-R17	Les cantons manquent de ressources pour la mise en œuvre du vote électronique.	28	Moyenne
ChF-VE-R18	L'utilisation effective du canal de vote électronique dépasse les limites de l'électorat autorisé (30% cantonal et 10% national).	39	Basse

Tableau 3 : Résumé de l'analyse et de l'évaluation des risques avant mitigation

Probabilité	Score d'impact: 32 – 49 (Haut)	Score d'impact: 22 – 31 (Moyen)	Score d'impact: 17 – 21 (Bas)
Haut		**R4** Campagne de dénigrement du vote électronique dans les médias (sociaux)	
Moyen	**R1** Faille sévère dans le système **R2** Défaut de détection des erreurs systématiques **R5** Achat de votes sur une plateforme anonyme **R6** Manipulation des votes par un état tiers **R7** Violation du secret du vote par un état tiers **R10** Autorisation d'un système défaillant **R11** Mise en œuvre d'un système différent de celui autorisé **R12** Mise en danger du développement des exigences de sécurité **R13** Manque d'experts indépendant	**R3** Manque d'acceptation du vote électronique **R8** Indisponibilité du système suite à une attaque par un état tiers **R16** Suppression du canal vocal en raison d'une coopération défaillante **R17** Suppression du canal de vote en raison d'un manque de ressources	
Bas	**R9** Exigences inadéquates **R14** Nouvelles technologies menaçant le secret du vote **R15** Perte du système pendant un scrutin **R18** Dépassement des plafonds légaux		

Tableau 4 : Carte des risques avant la mise en œuvre des mesures de mitigation

5 Traitement des risques

Une grande partie des mesures de mitigation des risques sont présentes dans les bases légales (ODP et OVotE). Cela n'est cependant pas suffisant et appelle une série de mesures complémentaires afin de réduire les risques à un niveau acceptable. Le tableau de traitement des risques suivant présente les mesures dites actuelles qui sont déjà mise en œuvre et les mesures dites futures qu'il est actuellement prévu de mettre en œuvre. Ces dernières comprennent notamment les mesures à moyen et long terme du catalogue de mesures de la Confédération et des cantons[20]. Les mesures futures seront complétées au fil du temps et selon les besoins dans une perspective d'amélioration continue des essais.

[20] www.bk.admin.ch > Droits politiques > Vote électronique > Essais de vote électronique

Score	Prob.	Action	Mesures actuelles	Mesures futures
ChF-VE-R1 Faille sévère dans le système				

40	Moyen	Mitiger	- Exigences légales :
			  - Contrôle indépendant des systèmes et des modalités d'exploitation (art. 27*l* ODP et art. 10 OVotE)
			  - Plafonds de 30% de l'électorat cantonal et 10% de l'électorat national (art. 27*f* ODP)
			  - Publicité des informations concernant le système et son exploitation (art. 27*l*[bis] ODP)
			  - Participation du public (art. 27*l*[ter] ODP)
			  - Établissement de la plausibilité (art. 27*i* al. 2 ODP)
			  - Recours à des experts indépendants et suivi scientifique (art. 27*o* ODP)
			  - Conditions à remplir pour obtenir l'agrément en vue de la tenue d'un scrutin électronique (art. 3 OVotE)
			  - Appréciation des risques (art. 4 OVotE)
			  - Exigences applicables à la vérifiabilité complète (art. 5 OVotE)
			  - Publication du code source et de la documentation du système et de son exploitation (art. 11 et 12 OVotE)
			  - Exigences applicables aux composants fiables au sens du ch. 2 et à leur exploitation (ch. 3 annexe OVotE)
			  - Vote à l'urne ou par correspondance toujours possible avant confirmation du vote (ch. 4.4 et 4.11 annexe OVotE)
			  - Détection et annonce d'incidents et de vulnérabilités en matière de sécurité; gestion des incidents en matière de sécurité et des améliorations (ch. 14 annexe OVotE)
			- Gestion d'un catalogue de mesures commun de la Confédération et des cantons
			- Convention de crise
			- Simulation de crise
				- Poursuite du développement du contrôle de la plausibilité des résultats du vote électronique (mesure B. 8 du catalogue de mesures)
				- Renforcement de la vérifiabilité (mesures A.4, A.5, A.6, A.19 et A.22 du catalogue de mesures)
				- Renforcement de la collaboration avec les milieux scientifiques et de l'accompagnement des essais par ces derniers (mesures D.1, D.2 et D.3 du catalogue de mesures
				- Poursuite du développement du système et de sa documentation (mesures A.9, A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 et A.25 du catalogue de mesures)
				- Extension des éléments du système dont le code source est publié (mesure A.11 du catalogue de mesures)
				- Amélioration de la documentation publiée (mesures A.17, A.20 et C.7 du catalogue de mesures)
				- Amélioration des capacités d'investigation (mesure B.13 du catalogue de mesures)
				- Amélioration de la documentation des appréciations des risques (mesures B.11 et B.12 du catalogue de mesures)

ChF-VE-R2 Défaut de détection des erreurs systématiques				

44	Moyen	Mitiger	- Exigences légales :
			  - Informations des votants (ch. 8 annexe OVotE)
			  - Détection et annonce d'incidents et de vulnérabilités en matière de sécurité; gestion des incidents en matière de sécurité et améliorations (ch. 14 annexe OVotE)
			- Convention de crise
			- Simulation de crise
				- Amélioration des capacités d'investigation (mesure B.13 du catalogue de mesures)

Score	Prob.	Action	Mesures actuelles	Mesures futures
ChF-VE-R3 Manque d'acceptation du vote électronique				

33	Moyen	Mitiger	- Exigences légales :
			  - Plafonds de 30% de l'électorat cantonal et 10% de l'électorat national (art. 27*f* ODP)
			  - Publicité des informations concernant le système et son exploitation (art. 27*l*[bis] ODP)
			  - Participation du public (art. 27*l*[ter] ODP)
			  - Informations des électeurs et publication des résultats du vote électronique (art. 27*m* ODP)
			  - Établissement de la plausibilité (art. 27*i* al. 2 ODP)
			  - Recours à des experts indépendants et suivi scientifique (art. 27*o* ODP)
			  - Conditions à remplir pour obtenir l'agrément en vue de la tenue d'un scrutin électronique (art. 3 OVotE)
			  - Appréciation des risques (art. 4 OVotE)
			  - Exigences applicables à la vérifiabilité complète (art. 5 OVotE)
			  - Publication du code source et de la documentation du système et de son exploitation (art. 11 et 12 OVotE)
			  - Responsabilité et compétences à l'égard du bon déroulement du scrutin électronique (art. 14 OVotE)
			- Organisation/participation à des événements publics
			- Mise à disposition de matériel d'information sur la sécurité du vote électronique
			- Gestion d'un catalogue de mesures commun de la Confédération et des cantons
			- Communication factuelle et transparente
			- Amélioration continue de la phase d'essai
				- Renforcement de la vérifiabilité (mesures A.4, A.5, A.6, A.19 et A.22 du catalogue de mesures)
				- Poursuite du développement du contrôle de la plausibilité des résultats du vote électronique (mesure B.8 du catalogue de mesures)
				- Renforcement de la collaboration avec les milieux scientifiques et de l'accompagnement des essais par ces derniers (mesures D.1, D.2 et D.3 du catalogue de mesures)
				- Poursuite du développement du système et de sa documentation (mesures A.9, A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 et A.25 du catalogue de mesures)
				- Extension des éléments du système dont le code source est publié (mesure A.11 du catalogue de mesures)
				- Amélioration de la documentation publiée (mesures A.17, A.20 et C.7 du catalogue de mesures)
				- Amélioration des capacités d'investigation (mesure B.13 du catalogue de mesures)
				- Amélioration de la documentation des appréciations des risques (mesures B.11 et B.12 du catalogue de mesures)

Score	Prob.	Action	Mesures actuelles	Mesures futures
ChF-VE-R4 Campagne de dénigrement du vote électronique dans les médias (sociaux)				

29	Haut	Mitiger	- Exigences légales :
			  - Publicité des informations concernant le système et son exploitation (art. 27*l*bis ODP)
			  - Participation du public (art. 27*l*ter ODP et art. 13 OVotE)
			  - Informations des électeurs et publication des résultats du vote électronique (art. 27*m* ODP)
			  - Recours à des experts indépendants et suivi scientifique (art. 27*o* ODP)
			  - Établissement de la plausibilité (art. 27*i* al. 2 ODP)
			  - Exigences applicables à la vérifiabilité complète (art. 5 OVotE)
			  - Contrôle indépendant des systèmes et des modalités d'exploitation (art. 27*l* ODP et art. 10 OVotE)
			  - Soumission des indicateurs aux vérificateurs (ch. 11.10 annexe OVotE)
			  - Élaboration d'un plan d'urgence (ch. 11.11 annexe OVotE)
			- Communication factuelle et transparente
			- Gestion d'un catalogue de mesures commun de la Confédération et des cantons
			- Convention de crise
			- Simulation de crise
				- Renforcement de la collaboration avec les milieux scientifiques et de l'accompagnement des essais par ces derniers (mesures D.1, D.2 et D.3 du catalogue de mesures)
				- Poursuite du développement du système et de sa documentation (mesures A.9, A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 et A.25 du catalogue de mesures)
				- Extension des éléments du système dont le code source est publié (mesure A.11 du catalogue de mesures)
				- Amélioration de la documentation publiée (mesures A.17, A.20 et C.7 du catalogue de mesures)
				- Amélioration des capacités d'investigation (mesure B.13 du catalogue de mesures)

ChF-VE-R5 Achat de votes sur une plateforme anonyme				

43	Moyen	Mitiger	- Exigences légales :
			  - Plafonds de 30% de l'électorat cantonal et 10% de l'électorat national (art. 27*f* ODP)
			  - Appréciation des risques (art. 4 OVotE)
			- Poursuite pénale du délit de corruption électorale également valable dans le cadre du vote électronique (art. 281 Code pénal suisse)	

Score	Prob.	Action	Mesures actuelles	Mesures futures
ChF-VE-R6 Manipulation des votes par un état tiers				

43	Moyen	Mitiger	- Exigences légales :
			  - Plafonds de 30% de l'électorat cantonal et 10% de l'électorat national (art. 27*f* ODP)
			  - Publicité des informations concernant le système et son exploitation (art. 27*l*[bis] ODP)
			  - Participation du public (art. 27*l*[ter] ODP)
			  - Établissement de la plausibilité (art. 27*i* al. 2 ODP)
			  - Recours à des experts indépendants et suivi scientifique (art. 27*o* ODP)
			  - Conditions à remplir pour obtenir l'agrément en vue de la tenue d'un scrutin électronique (art. 3 OVotE)
			  - Appréciation des risques (art. 4 OVotE)
			  - Exigences applicables à la vérifiabilité complète (art. 5 OVotE et ch. 2 annexe OVotE)
			  - Publication du code source et de la documentation du système et de son exploitation (art. 11 et 12 OVotE)
			  - Exigences applicables aux composants fiables au sens du ch. 2 et à leur exploitation (ch. 3 annexe OVotE)
			  - Vote à l'urne ou par correspondance toujours possible avant confirmation du vote (ch. 4.4 et 4.11 annexe OVotE)
			  - Exigences applicables aux imprimeries (ch. 7 annexe OVotE)
			  - Information et assistance (ch. 8 annexe OVotE)
			  - Détection et annonce d'incidents et de vulnérabilités en matière de sécurité; gestion des incidents en matière de sécurité et des améliorations (ch. 14 annexe OVotE)
			  - Fiabilité du personnel (ch. 20 annexe OVotE)
			  - Gestion de la communication et de l'exploitation (ch. 22 annexe OVotE)
			- Gestion d'un catalogue de mesures commun de la Confédération et des cantons
			- Veille en matière de menaces
			- Convention de crise
			- Simulation de crise
				- Renforcement de la vérifiabilité (mesures A.4, A.5, A.6, A.19 et A.22 du catalogue de mesures)
				- Poursuite du développement du contrôle de la plausibilité des résultats du vote électronique (mesure B. 8 du catalogue de mesures)
				- Poursuite du développement du système et de sa documentation (mesures A.9, A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 et A.25 du catalogue de mesures)
				- Amélioration des capacités d'investigation (mesure B.13 du catalogue de mesures)
				- Amélioration de la documentation des appréciations des risques (mesures B.11, et B.12 du catalogue de mesures)

Score	Prob.	Action	Mesures actuelles	Mesures futures
ChF-VE-R7 Violation du secret du vote par un état tiers				

38	Moyen	Mitiger	- Exigences légales :
			  - Plafonds de 30% de l'électorat cantonal et 10% de l'électorat national (art. 27*f* ODP)
			  - Appréciation des risques (art. 4 OVotE)
			  - Exigences applicables à la vérifiabilité complète (art. 5 OVotE et ch. 2 annexe OVotE)
			  - Exigences applicables aux composants fiables au sens du ch. 2 et à leur exploitation (ch. 3 annexe OVotE)
			  - Exigences applicables aux imprimeries (ch. 7 annexe OVotE)
			  - Information et assistance (ch. 8 annexe OVotE)
			  - Traitement des données confidentielles (ch. 12 OVotE)
			  - Détection et annonce d'incidents et de vulnérabilités en matière de sécurité; gestion des incidents en matière de sécurité et des améliorations (ch. 14 annexe OVotE)
			  - Fiabilité du personnel (ch. 20 annexe OVotE)
			- Gestion d'un catalogue de mesures commun de la Confédération et des cantons
			- Veille en matière de menaces
			- Convention de crise
			- Simulation de crise
				- Poursuite du développement du système et de sa documentation (mesures A.9, A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 et A.25 du catalogue de mesures)
				- Amélioration des capacités d'investigation (mesure B.13 du catalogue de mesures)
				- Amélioration de la documentation des appréciations des risques (mesures B.11 et B.12 du catalogue de mesures)

ChF-VE-R8 Indisponibilité du système suite à une attaque par un état tiers				

31	Moyen	Mitiger	- Exigences légales :
			  - Période de votation et d'élection de 3 à 4 semaines (art. 11 al. 3 et art. 33 al. 2 Loi fédérale sur les droits politiques)
			  - Appréciation des risques (art. 4 OVotE)
			  - Exigences applicables à la vérifiabilité complète (art. 5 OVotE et ch. 2 annexe OVotE)
			  - Exigences applicables aux composants fiables au sens du ch. 2 et à leur exploitation (ch. 3 annexe OVotE)
			  - Vote à l'urne ou par correspondance toujours possible avant confirmation du vote (ch. 4.4 et 4.11 annexe OVotE)
			  - Détection et annonce d'incidents et de vulnérabilités en matière de sécurité; gestion des incidents en matière de sécurité et des améliorations (ch. 14 annexe OVotE)
			  - Fiabilité du personnel (ch. 20 annexe OVotE)
			  - Gestion de la communication et de l'exploitation (ch. 22 annexe OVotE)
			- Gestion d'un catalogue de mesures commun de la Confédération et des cantons
			- Veille en matière de menaces
			- Convention de crise
			- Simulation de crise
				- Poursuite du développement du contrôle de la plausibilité des résultats du vote électronique (mesure B. 8 du catalogue de mesures)
				- Examiner les nouvelles mesures possibles de protection du réseau
				- Amélioration des capacités d'investigation (mesure B.13 du catalogue de mesures)

Score	Prob.	Action	Mesures actuelles	Mesures futures
ChF-VE-R9 Exigences inadéquates				
40	Bas	Mitiger	- Exigences légales : - Recours à des experts indépendants et suivi scientifique (art. 27*o* ODP) - Organisation/participation à des événements publics - Exigences techniques documentées dans une ordonnance de la ChF pour être plus rapidement adaptables - Veille technologique, sociologique et légale dans le domaine du vote électronique - Veille en matière de sécurité de l'information - Collaboration avec les milieux scientifiques	- Renforcement de la collaboration avec les milieux scientifiques et de l'accompagnement des essais par ces derniers (mesures D.1, D.2 et D.3 du catalogue de mesures)
ChF-VE-R10 Autorisation d'un système défaillant				

47	Moyen	Mitiger	- Exigences légales :
			  - Plafonds de 30% de l'électorat cantonal et 10% de l'électorat national (art. 27*f* ODP)
			  - Contrôle des systèmes et des modalités d'exploitation (art. 27*l* ODP et art. 10 OVotE)
			  - Publication du code source et de la documentation du système et de son exploitation (art. 11 et 12 OVotE)
			  - Participation du public (art. 13 OVotE)
			  - Détection et annonce d'incidents et de vulnérabilités en matière de sécurité; gestion des incidents en matière de sécurité et des améliorations (ch. 14 annexe OVotE)
			  - Développement et maintenance de systèmes d'information (ch. 24 annexe OVotE)
			  - Qualité du code source et de la documentation (ch. 25 annexe OVotE)
			- Gestion d'un catalogue de mesures commun de la Confédération et des cantons
				- Renforcement de la collaboration avec les milieux scientifiques et de l'accompagnement des essais par ces derniers (mesures D.1, D.2 et D.3 du catalogue de mesures)
				- Poursuite du développement du contrôle de la plausibilité des résultats du vote électronique (mesure B. 8 du catalogue de mesures)
				- Poursuite du développement du système et de sa documentation (mesures A.9, A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 et A.25 du catalogue de mesures)
				- Amélioration des capacités d'investigation (mesure B.13 du catalogue de mesures)

ChF-VE-R11 Mise en œuvre d'un système différent de celui autorisé				

44	Moyen	Mitiger	- Exigences légales :
			  - Publication d'une pièce justificative attestant que les programmes lisibles par machine ont été créés au moyen du code source du logiciel tel qu'il a été publié (art. 27*l*^{bis}, al. 2, let. d ODP et art. 11, al. 1, let b OVotE)
			  - Définition et approbation des rôles et accès (ch. 18, 21 et 23 annexe OVotE)
			  - Compilation et déploiement fiables et vérifiables (ch. 24.3 annexe OVotE)	

Score	Prob.	Action	Mesures actuelles	Mesures futures
ChF-VE-R12 Mise en danger du développement des exigences de sécurité				
40	Moyen	Mitiger	- Exigences légales : - Recours à des experts indépendants et suivi scientifique (art. 27*o* ODP) - Organisation/participation à des événements publics - Veille technologique, sociologique et légale dans le domaine du vote électronique - Veille en matière de sécurité de l'information - Collaboration avec les milieux scientifiques	- Renforcement de la collaboration avec les milieux scientifiques et de l'accompagnement des essais par ces derniers (mesures D.1, D.2 et D.3 du catalogue de mesures)
ChF-VE-R13 Manque d'experts indépendants				
32	Moyen	Mitiger	- Exigences légales : - Recours à des experts indépendants et suivi scientifique (art. 27*o* ODP) - Organisation/participation à des événements publics - Collaboration avec les milieux scientifiques	- Renforcement de la collaboration avec les milieux scientifiques et de l'accompagnement des essais par ces derniers (mesures D.1, D.2 et D.3 du catalogue de mesures)
ChF-VE-R14 Nouvelles technologies menaçant le secret du vote				
35	Bas	Surveiller	- Veille technologique, sociologique et légale dans le domaine du vote électronique - Veille en matière de sécurité de l'information - Collaboration avec les milieux scientifiques	- Renforcement de la collaboration avec les milieux scientifiques et de l'accompagnement des essais par ces derniers (mesures D.1, D.2 et D.3 du catalogue de mesures) - Poursuite du développement du système et de sa documentation (mesures A.9, A.10, A.12, A.13, A.14, A.15, A.16, A.18, A.21, A.23, A.24 et A.25 du catalogue de mesures)
ChF-VE-R15 Perte du système pendant un scrutin				

40	Bas	Mitiger	- Exigences légales :
			  - Période de votation et d'élection de 3 à 4 semaines (art. 11 al. 3 et art. 33 al. 2 Loi fédérale sur les droits politiques)
			  - Plafonds de 30% de l'électorat cantonal et 10% de l'électorat national (art. 27*f* ODP)
			- Vote à l'urne ou par correspondance
			- Convention de crise
			- Simulation de crise	

ChF-VE-R16 Suppression du canal vocal en raison d'une coopération défaillante				
23	Moyen	Mitiger	- Gestion d'un catalogue de mesures commun de la Confédération et des cantons - À court terme : cofinancement des mesures dont les coûts sont principalement supportés par les (quelques) cantons concernés par le biais des instruments existants de la Confédération (p. ex. Administration Numérique Suisse ANS) - À moyen et long terme : garantie du financement à long terme - Coordination des travaux par le biais des organes de projet existants	- Examen à long terme des processus, rôles et des tâches (mesure B.10 du catalogue de mesures)

Score	Prob.	Action	Mesures actuelles	Mesures futures
ChF-VE-R17 Suppression du canal de vote en raison d'un manque de ressources				
28	Moyen	Mitiger	- À court terme : cofinancement des mesures dont les coûts sont principalement supportés par les (quelques) cantons concernés, par le biais des instruments existants de la Confédération (p. ex. ANS) - À moyen et long terme : garantie du financement à long terme - Gestion d'un catalogue de mesures commun de la Confédération et des cantons	- Examen à long terme des processus, rôles et des tâches (mesure B.10 du catalogue de mesures)
ChF-VE-R18 Dépassement des plafonds légaux				
39	Bas	Mitiger	- Exigences légales : - Autorisation générale octroyée par le Conseil fédéral (art. 27*a* et 27*c* ODP) - Échanges constants avec les cantons - Accompagnement des essais par la ChF	

Tableau 5 : Mesures actuelles et futures prises pour le traitement des risques

6 Risques résiduels

Les risques résiduels sont entendus comme les risques qui subsistent après la mise en œuvre des différentes mesures de mitigation définies au chapitre 5. Ces derniers doivent faire l'objet d'une acceptation explicite ou de mesures supplémentaires de surveillance quand leur niveau ne leur permet pas d'être accepté. La table ci-dessous en présente un condensé.

Action	Risque résiduel et justification	Score	Prob.	Décision
ChF-VE-R1 Faille sévère dans le système				
Mitiger	Un grand nombre de mesures sont mises en œuvre pour éviter à des failles sévères de subsister une fois le système mis en service. Le risque zéro n'existe cependant pas en la matière. Les mesures de protection (cryptographiques, techniques et organisationnelles) forment des couches qui se superposent les unes aux autres. Ainsi, un défaut dans l'une de ses mesures n'implique pas forcément qu'une attaque puisse être menée avec succès.	17	Bas	Accepté
ChF-VE-R2 Défaut de détection des erreurs systématiques				
Mitiger	Les cantons ont intégré les retours des votants dans leurs processus et disposent d'un plan d'action en cas d'incident de ce genre. De plus, la convention de crise et l'exercice de scénarios de crise offrent un bon vecteur de sensibilisation. Il reste toujours possible que l'un ou l'autre canton oublie de rapporter de tels cas mais plus il y aura de cantons participants, moins ce risque sera élevé. Les informations transmises aux électeurs leur demandant explicitement de vérifier leurs codes et le canal mis à leur disposition pour rapporter les cas de code erronés permet d'augmenter la détection des fraudes et devrait permettre aux votants touchés de se rendre compte du problème, de ne pas confirmer leur vote et de se tourner vers un autre canal de vote.	34	Bas	Surveillé
ChF-VE-R3 Manque d'acceptation du vote électronique				
Mitiger	Les facteurs affectant l'acceptation d'un nouveau canal de vote sont un domaine de recherche à part entière. C'est en conduisant des essais dans un cadre contraint tel que défini que ces recherches sont possibles. Cette démarche parait raisonnable tant du point de vue de son utilité que de l'impact qu'elle peut avoir sur les scrutins. En effet, les essais sont conduits sur une part limitée de l'électorat, ce qui permet une amélioration continue des processus et des outils avec un accompagnement par les milieux scientifiques. De plus, la communication factuelle mise en place devrait permettre à chacun de se faire une idée objective de la situation et la vérifiabilité contribue significativement à la garantie du secret du vote et à l'établissement de résultats fiables. Malgré les mesures de mitigation mises en place, il se peut toutefois que l'inclusion de moyens informatiques dans le processus de vote soit rédhibitoire pour une certaine partie des électeurs. Il n'en reste pas moins que les récentes études[21] en la	28	Bas	Surveillé

[21] Étude nationale sur la cyberadministration 2022 – Compte rendu (https://www.administration-numerique-suisse.ch/application/files/3416/5216/3445/Etude_nationale_sur_la_cyberadministration_2022_compte_rendu.pdf)

Étude Deloitte 2021 sur le gouvernement numérique en Suisse : Les moteurs et les freins des services de cyberadministration en Suisse en 2021 (https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/public-sector/deloitte-ch-fr-digital-government-study-1-2.pdf)

Rapport final de l'enquête auprès de la population sur le thème de la participation politique et de la numérisation à Bâle-Ville de 2020 (https://www.bs.ch/dam/jcr:96cfb1f0-96f8-4ec0-bbf1-3f566daa1247/2020-Bevoelkerungsbefragung-Digitalisierung-und-Politik-Kanton-Basel-Stadt.pdf)

Étude nationale sur la cyberadministration 2019 – Compte rendu (https://www.administration-numerique-suisse.ch/application/files/6416/3895/8851/Etude-nationale-sur-la-cyberadministration-2019-compte-rendu.pdf)

Action	Risque résiduel et justification	Score	Prob.	Décision
	matière montrent une demande pour le canal de vote électronique.			
ChF-VE-R4 Campagne de dénigrement du vote électronique dans les médias (sociaux)				
Mitiger	Une communication continue, factuelle et transparente est la meilleure technique pour contrer une communication biaisée. Si elle ne permet pas de convaincre ceux qui ont déjà un parti pris, elle devrait permettre à chacun de se faire une idée objective de la situation. La convention de crise règle les aspects de communication et les exercices assurent que la convention est suivie en cas de crise.	17	Moyen	Accepté
ChF-VE-R5 Achat de votes sur une plateforme anonyme				
Mitiger	Le système ne fournit pas de preuve de vote au votant qu'il pourrait ensuite utiliser pour démonter à un acheteur n'ayant pas accès (ni directement, ni indirectement, p. ex. par des employés) au système qu'il a voté comme demandé. Ce dernier ne peut donc avoir de garantie dans un tel cas, ce qui devrait le décourager. Il reste le cas de l'électeur vendant son matériel de vote. Cependant, la limitation de l'électorat autorisé devrait réduire l'intérêt de ce type d'attaque et en réduit en tous cas la portée. Dans tous les cas, la poursuite pénale des fraudes électorales et de la corruption électorale est possible.	17	Moyen	Surveillé
ChF-VE-R6 Manipulation des votes par un état tiers				
Mitiger	Un grand nombre de mesures sont mises en œuvre pour éviter ce risque. La vérifiabilité, en particulier, empêche qu'une telle manipulation puisse être mise en œuvre sans être détectée. Bien que la cryptographie couvrant la vérifiabilité fait l'objet d'un examen étendu par le public et les experts, il reste cependant le risque d'une défaillance dans sa conception ou sa mise en œuvre. Cependant l'exploitation d'une telle faille demanderait un effort démesuré pour un faible gain du fait, en particulier, de la limitation de l'électorat. Il est en outre prévu de renforcer la vérifiabilité et la collaboration avec les milieux scientifiques pendant la phase d'essai. De plus, et afin d'éviter un vol des codes, il est exigé des imprimeries qu'elles prennent des mesures de protection de ces derniers, que ce soit pendant ou après leur impression. En résumé, les mesures mises en œuvre, dont la limitation de l'électorat, font du vote électronique un angle d'attaque peu intéressant pour qui voudrait manipuler les résultats. L'effort nécessaire à une attaque est disproportionné par rapport à l'effet qu'elle pourrait avoir, sans compter le risque de se faire détecter.	30	Bas	Accepté
ChF-VE-R7 Violation du secret du vote par un état tiers				
Mitiger	Toutes les mesures techniques possibles et raisonnables sont mises en œuvre pour éviter qu'une seule personne puisse réunir toutes les informations permettant de violer massivement le secret du vote. Une attaque directe de l'ordinateur du votant, en espionnant ses clics, pourrait toujours révéler son vote mais la sensibilisation de la population à l'utilisation de moyens électroniques pour des opérations sensibles va grandissante et on peut attendre des votants électroniques qu'ils assument la responsabilité de la conformité de l'appareil qu'ils utilisent avec les bonnes pratiques en matière de sécurité. De plus, selon l'utilisation que les votants font d'autres instruments (p. ex. médias	20	Moyen	Accepté

Action	Risque résiduel et justification	Score	Prob.	Décision
	sociaux), ils peuvent offrir des moyens bien plus accessibles de déduire si et comment ils ont voté. La limitation de l'électorat autorisé devrait également réduire l'intérêt de ce type d'attaque.			
ChF-VE-R8 Indisponibilité du système suite à une attaque par un état tiers				
Mitiger	L'infrastructure du système doit être protégée contre les attaques de type « déni de service » mais celle des votants ne le doit pas. Une attaque individuelle de ce type ne peut donc être écartée. Toutefois, le vote à l'urne reste toujours possible. Les manœuvres d'influence d'états tiers ne se limitent pas au vote électronique et font déjà l'objet de réflexions et d'actions plus globales.	17	Moyen	Accepté
ChF-VE-R9 Exigences inadéquates				
Mitiger	Un dialogue constant avec les milieux scientifiques et professionnels et la participation aux événements dédiés au vote électronique devrait permettre de maintenir à niveau les connaissances et par là garder une base légale pertinente ou à tout le moins permettre de se rendre compte de l'inadéquation de cette dernière. Les différentes veilles remplissent la même fonction. Le fait que les aspects techniques et donc les plus susceptibles d'évoluer, soient dans une ordonnance de la ChF permet une plus grande flexibilité pour leur mise à jour.	30	Bas	Accepté
ChF-VE-R10 Autorisation d'un système défaillant				
Mitiger	Les contrôles indépendant et public des systèmes et de leur modalité d'exploitation, s'ils ne permettent pas totalement d'exclure la présence de faille, n'en sont pas moins efficaces pour leur prévention. Les essais sont menés dans un cadre restreint, ce qui permet de limiter l'impact sur le scrutin si l'une ou l'autre des exigences devait ne pas être remplie tout en permettant une amélioration continue des processus et des outils. De plus, les mesures liées au monitoring et à la gestion des incidents devraient permettre une investigation efficace des éventuels cas.	27	Bas	Accepté
ChF-VE-R11 Mise en œuvre d'un système différent de celui autorisé				
Mitiger	Les exigences relatives à la compilation et au déploiement fiables et vérifiables permettent de s'assurer que le système utilisé correspond à celui qui a été contrôlé. Elles ne permettent cependant pas d'exclure la possibilité d'une intervention volontaire malveillante après l'installation. Les accès étant contrôlés et faisant l'objet d'une collecte de traces, une telle intervention ne devrait pas pouvoir passer inaperçue.	44	Bas	Surveillé
ChF-VE-R12 Mise en danger du développement des exigences de sécurité				
Mitiger	Le fait d'encourager et de financer la recherche permet de maintenir un intérêt pour le domaine. De même en ce qui concerne l'intégration des milieux scientifiques et la collaboration avec ces derniers. Les différentes veilles permettent également de profiter des avancées qui se feraient en dehors du périmètre d'action de la ChF.	18	Bas	Accepté
ChF-VE-R13 Manque d'experts indépendants				
Mitiger	La participation aux événements en lien avec le vote électronique permet à la ChF de garder une vue sur les experts du domaine et leurs compétences. Elle ne garantit cependant pas qu'ils acceptent de participer au contrôle indépendant des systèmes de vote électronique.	32	Bas	Surveillé

Action	Risque résiduel et justification	Score	Prob.	Décision
ChF-VE-R14 Nouvelles technologies menaçant le secret du vote				
Surveiller	Nul ne peut prévoir le futur. Ce risque ne peut être mitigé au-delà d'une surveillance technologique et la mise en œuvre de mesures techniques, quand celles-ci seront disponibles et nécessaires.	35	Bas	Surveillé
ChF-VE-R15 Perte du système pendant un scrutin				
Mitiger	La convention de crise prévoit un tel cas et apporte des pistes à la résolution de ce problème sans pouvoir le prévenir. Le fait que le fournisseur actuel soit la Poste, une entreprise aux mains de l'état, apporte cependant de solides garanties dans ce domaine.	30	Bas	Accepté
ChF-VE-R16 Suppression du canal vocal en raison d'une coopération défaillante				
Mitiger	La Confédération n'étant pas partie aux contrats qui lient les cantons à leurs fournisseurs, elle ne peut pas agir à ce niveau. Les organes de projet incluant les différents acteurs permettent d'anticiper et de discuter les éventuelles difficultés. Finalement, la participation de la Confédération au financement de la mise en œuvre par les cantons peut également alléger certaines de ces difficultés.	23	Bas	Accepté
ChF-VE-R17 Suppression du canal de vote en raison d'un manque de ressources				
Mitiger	Le vote électronique fait partie du Plan de mise en œuvre de l'ANS. Cette dernière soutient ainsi les cantons dans l'adoption du vote électronique. Une réévaluation à long terme des rôles et des tâches pourrait potentiellement alléger la charge des cantons.	28	Bas	Accepté
ChF-VE-R18 Dépassement des plafonds légaux				
Mitiger	Les cantons sont en charge des scrutins pour tous les canaux de vote. Ils mettent en place les mesures nécessaires au contrôle de l'accès au vote électronique (p. ex. enregistrement préalable, limitation à l'électorat de certaines communes). La procédure d'autorisation et d'agrément permet de contrôler l'électorat national autorisé.	27	Bas	Accepté

Tableau 6 : Risques résiduels et décision finale

Probabilité	Score d'impact: 32 – 49 (Haut)	Score d'impact: 22 – 31 (Moyen)	Score d'impact: 17 – 21 (Bas)
Haut			
Moyen			**R4** Campagne de dénigrement du vote électronique dans les médias (sociaux) **R5** Achat de votes sur une plateforme anonyme **R7** Violation du secret du vote par un état tiers **R8** Indisponibilité du système suite à une attaque par un état tiers
Bas	**R2** Défaut de détection des erreurs systématiques **R11** Mise en œuvre d'un système différent de celui autorisé **R13** Manque d'experts indépendant **R14** Nouvelles technologies menaçant le secret du vote	**R3** Manque d'acceptation du vote électronique **R6** Manipulation des votes par un état tiers **R9** Exigences inadéquates **R10** Autorisation d'un système défaillant **R15** Perte du système pendant un scrutin **R16** Suppression du canal vocal en raison d'une coopération défaillante **R17** Suppression du canal de vote en raison d'un manque de ressources **R18** Dépassement des plafonds légaux	**R1** Faille sévère dans le système **R12** Mise en danger du développement des exigences de sécurité

Tableau 7 : Carte des risques résiduels après la mise en œuvre des mesures de mitigation

Validé par la Chancellerie fédérale :

Walter Thurnherr
Chancelier de la Confédération

Signature :

Thurnherr Walter CW0DQJ
01.03.2023

Info: admin.ch/esignature | validator.ch

Barbara Perriard
Cheffe de la Section des droits politiques

Signature :

Perriard Barbara Z5IT5Z
01.03.2023

Info: admin.ch/esignature | validator.ch

Aurore Borer
Cheffe de projet partiel Vote électronique

Signature :

Borer Aurore HXCUTE
01.03.2023

Info: admin.ch/esignature | validator.ch

Annexe I Évaluation détaillée des risques

ChF-VE-R1 Faille sévère dans le système

Menace	Une faille de sécurité sévère affectant le système est découverte pendant le scrutin
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés
Conséquences	Le canal de vote électronique doit être suspendu et une investigation menée pour déterminer l'impact de la faille et si elle a été exploitée. Si la faille a été exploitée et qu'il n'est pas possible de démontrer quel vote est légitime et quel vote ne l'est pas, l'ensemble des bulletins de vote électronique doit être écarté. Si le résultat du vote avait pu changer en raison de ces votes, un recours pourrait conduire à l'annulation du scrutin. La réputation des autorités serait grandement affectée. Les essais de vote électronique pourraient être suspendus.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Moyenne		Basse	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Haut (3)	15	Bas (1)	5
Légal	Haut (3)	15	Bas (1)	5
Viabilité	Moyen (2)	6	Bas (1)	3
Finance	Bas (1)	3	Bas (1)	3
Ressources	Bas (1)	1	Bas (1)	1
Score d'impact		**40**		**17**

ChF-VE-R2 Défaut de détection des erreurs systématiques

Menace	Des signalements de codes de vérification erronés sont faits dans plusieurs cantons mais aucune alerte n'est lancée au niveau national faute de coordination entre les cantons et la ChF
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie
Conséquences	Comme le problème n'a pas été identifié, les investigations nécessaires n'ont pas pu être lancée en temps opportun et les votants n'ont pas pu être rendus encore plus attentifs à l'importance particulière de vérifier les codes de vérification en l'absence de détection du problème. Les votants n'ayant pas vérifié leurs codes de vérification ont pu confirmer un vote qui ne représentait pas leur intention. Il est si difficile de différencier les votes légitimes de votes manipulés que l'ensemble des bulletins de vote électronique doit être écarté. Si le résultat du vote avait pu changer en raison de ces votes, un recours pourrait conduire à l'annulation du scrutin. La réputation des autorités serait grandement affectée. Les essais de vote électronique pourraient être suspendus.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Moyenne		Basse	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Haut (3)	15	Moyen (2)	10
Légal	Haut (3)	15	Moyen (2)	10
Viabilité	Moyen (2)	6	Moyen (2)	6
Finance	Moyen (2)	6	Moyen (2)	6
Ressources	Moyen (2)	2	Moyen (2)	2
Score d'impact		**44**		**34**

ChF-VE-R3	***Manque d'acceptation du vote électronique***
Menace	Le vote électronique n'est pas suffisamment accepté.
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie
Conséquences	Soit le canal de vote n'est simplement pas utilisé, soit il l'est mais les résultats qu'il produit ne sont pas acceptés par une grande partie de la population.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Moyenne		Basse	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Haut (3)	15	Moyen (2)	10
Légal	Bas (1)	5	Bas (1)	5
Viabilité	Haut (3)	9	Haut (3)	9
Finance	Bas (1)	3	Bas (1)	3
Ressources	Bas (1)	1	Bas (1)	1
Score d'impact		**33**		**28**

ChF-VE-R4	***Campagne de dénigrement du vote électronique dans les médias (sociaux)***
Menace	Une campagne de dénigrement du vote électronique est lancée sur les réseaux sociaux ou dans les médias. Celle-ci peut se baser sur des événements en lien avec le vote électronique à l'étranger, le supposé manque de contrôle public des processus de vote, de fausses allégations relatives aux mécanismes de la vérifiabilité ou une communication défaillante des autorités.
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie
Conséquences	Si un scrutin est en cours, la confiance des électeurs risque de gravement chuter, les détournant ainsi du canal de vote électronique. De plus, une mauvaise communication pourrait également nuire à la crédibilité des autorités. Finalement, des recours seront possibles.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Haute		Moyenne	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Moyen (2)	10	Bas (1)	5
Légal	Bas (1)	5	Bas (1)	5
Viabilité	Moyen (2)	6	Bas (1)	3
Finance	Moyen (2)	6	Bas (1)	3
Ressources	Moyen (2)	2	Bas (1)	1
Score d'impact		**29**		**17**

ChF-VE-R5	***Achat de votes sur une plateforme anonyme***
Menace	Une campagne d'achat de votes est lancée et propose une plateforme en ligne permettant aux électeurs de vendre leur vote
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés f. il est impossible de faire un usage abusif des preuves relatives au comportement de vote
Conséquences	La plateforme permet une vente anonyme, il est donc très difficile d'identifier les personnes qui ont vendu leur vote. De plus, il n'est pas possible d'identifier ces votes dans l'urne et l'ensemble des bulletins de vote électronique doit donc être écarté. Si le résultat du vote avait pu changer en raison de ces votes, un recours pourrait conduire à l'annulation du scrutin. La réputation des autorités serait grandement affectée. Les essais de vote électronique seraient très probablement suspendus.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Moyenne		Moyenne	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Haut (3)	15	Bas (1)	5
Légal	Haut (3)	15	Bas (1)	5
Viabilité	Haut (3)	9	Bas (1)	3
Finance	Bas (1)	3	Bas (1)	3
Ressources	Bas (1)	1	Bas (1)	1
Score d'impact		**43**		**17**

ChF-VE-R6	***Manipulation des votes par un état tiers***
Menace	Un état tiers mobilise ses services et réussi à manipuler les votes dans le système
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie
Conséquences	Le canal de vote électronique doit être suspendu et une investigation menée pour déterminer quel vote est légitime et quel vote ne l'est pas. Si ce n'est pas possible, l'ensemble des bulletins de vote électronique doit être écarté. Si le résultat du vote avait pu changer en raison de ces votes, un recours pourrait conduire à l'annulation du scrutin. La réputation des autorités serait grandement affectée. Les essais de vote électronique seraient très probablement suspendus. Si la manipulation n'est pas détectée, une décision allant contre la volonté du peuple aura pu être prise.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Moyenne		Basse	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Haut (3)	15	Moyen (2)	10
Légal	Haut (3)	15	Moyen (2)	10
Viabilité	Haut (3)	9	Moyen (2)	6
Finance	Bas (1)	3	Bas (1)	3
Ressources	Bas (1)	1	Bas (1)	1
Score d'impact		**43**		**30**

ChF-VE-R7	***Violation du secret du vote par un état tiers***
Menace	Un état tiers mobilise ses services et réussi à violer le secret du vote
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés f. il est impossible de faire un usage abusif des preuves relatives au comportement de vote
Conséquences	L'état en question peut utiliser ces informations contre les votants à plus ou moins long terme. Il peut également vendre ces informations à d'autres états ou des groupes malveillants qui peuvent ensuite les utiliser au détriment des votants. L'affaire devient publique et la confiance dans le canal de vote électronique et dans les autorités est gravement entachée. Les essais de vote électronique devront être suspendus.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Moyenne		Moyenne	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Haut (3)	15	Bas (1)	5
Légal	Moyen (2)	10	Bas (1)	5
Viabilité	Haut (3)	9	Moyen (2)	6
Finance	Bas (1)	3	Bas (1)	3
Ressources	Bas (1)	1	Bas (1)	1
Score d'impact		**38**		**20**

ChF-VE-R8	***Indisponibilité du système suite à une attaque par un état tiers***
Menace	Un état tiers mobilise ses services et réussit à influencer le résultat du scrutin en excluant des votants
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie c. le vote électronique est accessible et opérationnel
Conséquences	Les attaques peuvent rendre le système indisponible pour tout ou partie de l'électorat et de ce fait l'exclure. Les votants suisses vivant à l'étranger ne pourront pas soumettre leur vote à temps. Il se peut que cela conduise à des recours contre les résultats du scrutin. Le vote électronique sera probablement remis en question étant donné que l'un de ses groupes cibles a été particulièrement touché par l'attaque.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Moyenne		Moyenne	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Moyen (2)	10	Bas (1)	5
Légal	Moyen (2)	10	Bas (1)	5
Viabilité	Moyen (2)	6	Bas (1)	3
Finance	Bas (1)	3	Bas (1)	3
Ressources	Moyen (2)	2	Bas (1)	1
Score d'impact		**31**		**17**

ChF-VE-R9	***Exigences inadéquates***
Menace	Exigences inadéquates qui ne permettent plus de maintenir le niveau de sécurité voulu
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés c. le vote électronique est accessible et opérationnel d. les informations personnelles des électeurs sont protégées e. les informations destinées aux électeurs sont protégées contre les manipulations f. il est impossible de faire un usage abusif des preuves relatives au comportement de vote
Conséquences	Le système et son exploitation peuvent être plus facile à compromettre et la critique ne manquera pas de se renforcer dans le public et dans les médias. La réputation des autorités serait grandement affectée et la poursuite des essais remise en question.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Basse		Basse	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Haut (3)	15	Moyen (2)	10
Légal	Haut (3)	15	Moyen (2)	10
Viabilité	Moyen (2)	6	Moyen (2)	6
Finance	Bas (1)	3	Bas (1)	3
Ressources	Bas (1)	1	Bas (1)	1
Score d'impact		**40**		**30**

ChF-VE-R10	***Autorisation d'un système défaillant***
Menace	La Confédération a autorisé l'utilisation d'un système dont les mesures de sécurité ne satisfont pas les exigences légales.
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés c. le vote électronique est accessible et opérationnel d. les informations personnelles des électeurs sont protégées e. les informations destinées aux électeurs sont protégées contre les manipulations f. il est impossible de faire un usage abusif des preuves relatives au comportement de vote
Conséquences	Si un usage abusif du système ne peut être écarté et que la participation électronique peut changer le résultat du scrutin, le scrutin devra très probablement être déclaré nul. La réputation des autorités sera gravement entachée et les essais de vote électronique devront être suspendus.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Moyenne		Basse	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Haut (3)	15	Moyen (2)	10
Légal	Haut (3)	15	Moyen (2)	10
Viabilité	Haut (3)	9	Bas (1)	3
Finance	Moyen (2)	6	Bas (1)	3
Ressources	Moyen (2)	2	Bas (1)	1
Score d'impact		**47**		**27**

ChF-VE-R11	***Mise en œuvre d'un système différent de celui autorisé***
Menace	Déploiement et utilisation d'un système différent de celui autorisé
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés c. le vote électronique est accessible et opérationnel d. les informations personnelles des électeurs sont protégées e. les informations destinées aux électeurs sont protégées contre les manipulations f. il est impossible de faire un usage abusif des preuves relatives au comportement de vote
Conséquences	Le système n'aura pas fait l'objet d'un contrôle indépendant ni d'une observation publique. Il n'y aura donc aucune garantie quant à la présence ou non de failles. Si les votes soumis par voie électronique avaient pu changer le résultat du scrutin, un recours pourrait entrainer son annulation. La réputation des autorités en serait grandement affectée.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Moyenne		Basse	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Haut (3)	15	Haut (3)	15
Légal	Haut (3)	15	Haut (3)	15
Viabilité	Moyen (2)	6	Moyen (2)	6
Finance	Moyen (2)	6	Moyen (2)	6
Ressources	Moyen (2)	2	Moyen (2)	2
Score d'impact		**44**		**44**

ChF-VE-R12	***Mise en danger du développement des exigences de sécurité***
Menace	Désintérêt des experts pour le vote électronique qui conduit à une stagnation puis une obsolescence des exigences de sécurité
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés c. le vote électronique est accessible et opérationnel d. les informations personnelles des électeurs sont protégées e. les informations destinées aux électeurs sont protégées contre les manipulations f. il est impossible de faire un usage abusif des preuves relatives au comportement de vote
Conséquences	Les experts ne font plus de recherches sur le sujet du vote électronique et ne souhaitent pas être associés aux travaux. Les essais de vote électronique ne pourront être poursuivi dans de bonnes conditions et devront très probablement être suspendus.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Moyenne		Basse	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Moyen (2)	10	Bas (1)	5
Légal	Moyen (2)	10	Bas (1)	5
Viabilité	Haut (3)	9	Bas (1)	3
Finance	Haut (3)	9	Bas (1)	3
Ressources	Moyen (2)	2	Moyen (2)	2
Score d'impact		**40**		**18**

ChF-VE-R13 Manque d'experts indépendants

Menace	Manque d'experts indépendants qualifiés pour la conduite des contrôles
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés c. le vote électronique est accessible et opérationnel d. les informations personnelles des électeurs sont protégées e. les informations destinées aux électeurs sont protégées contre les manipulations f. il est impossible de faire un usage abusif des preuves relatives au comportement de vote
Conséquences	Le contrôle des systèmes doit être différé, reportant d'autant la possibilité de les mettre en œuvre. À terme, ceci peut décourager les cantons et les fournisseurs de système et donc stopper les essais de vote électronique.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Moyenne		Basse	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Moyen (2)	10	Moyen (2)	10
Légal	Bas (1)	5	Bas (1)	5
Viabilité	Moyen (2)	6	Moyen (2)	6
Finance	Haut (3)	9	Haut (3)	9
Ressources	Moyen (2)	2	Moyen (2)	2
Score d'impact		**32**		**32**

ChF-VE-R14 Nouvelles technologies menaçant le secret du vote

Menace	Développement à large échelle d'une nouvelle technologie rendant obsolètes les exigences de sécurité en matière de protection du secret du vote (p. ex. ordinateur quantique)
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés
Conséquences	Le système et son exploitation peuvent être plus facile à compromettre et la critique ne manquera pas de se renforcer dans le public et dans les médias. La réputation des autorités serait affectée et la poursuite des essais remise en question.

Évaluation

	Initiale		**Après mitigation**
Probabilité	Basse		Pas de changement car le risque est surveillé sans que d'autres mesures ne soient prises
Critères	**Valeur**	**Score**	
Réputation et confiance	Moyen (2)	10	
Légal	Haut (3)	15	
Viabilité	Moyen (2)	6	
Finance	Bas (1)	3	
Ressources	Bas (1)	1	
Score d'impact		**35**	

ChF-VE-R15 Perte du système pendant un scrutin

Menace	Le fournisseur de système n'est plus en mesure de fournir son système pendant un scrutin alors que des votes ont déjà été émis
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie c. le vote électronique est accessible et opérationnel
Conséquences	Les votes émis de manière électronique sont définitivement perdus. Si le résultat du vote avait pu changer en raison de ces votes, un recours pourrait conduire à l'annulation du scrutin. La réputation des autorités serait grandement affectée. Les essais de vote électronique pourraient être suspendus.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Basse		Basse	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Haut (3)	15	Moyen (2)	10
Légal	Haut (3)	15	Moyen (2)	10
Viabilité	Moyen (2)	6	Moyen (2)	6
Finance	Bas (1)	3	Bas (1)	3
Ressources	Bas (1)	1	Bas (1)	1
Score d'impact		**40**		**30**

ChF-VE-R16 Suppression du canal vocal en raison d'une coopération défaillante

Menace	Des différends nuisent à la coopération entre les autorités et les fournisseurs de systèmes, de sorte que le vote électronique ne peut plus être développé ou est interrompu.
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	c. le vote électronique est accessible et opérationnel
Conséquences	Les essais de vote électronique ne sont plus possibles.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Moyenne		Basse	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Bas (1)	5	Bas (1)	5
Légal	Bas (1)	5	Bas (1)	5
Viabilité	Haut (3)	9	Haut (3)	9
Finance	Bas (1)	3	Bas (1)	3
Ressources	Bas (1)	1	Bas (1)	1
Score d'impact		**23**		**23**

ChF-VE-R17 Suppression du canal de vote en raison d'un manque de ressources

Menace	Les cantons manquent de ressources pour la mise en œuvre du vote électronique.
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	c. le vote électronique est accessible et opérationnel
Conséquences	Le vote électronique est abandonné par les cantons, suspendant ainsi les essais.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Moyenne		Basse	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Moyen (2)	10	Moyen (2)	10
Légal	Bas (1)	5	Bas (1)	5
Viabilité	Haut (3)	9	Haut (3)	9
Finance	Bas (1)	3	Bas (1)	3
Ressources	Bas (1)	1	Bas (1)	1
Score d'impact		**28**		**28**

ChF-VE-R18	***Dépassement des plafonds légaux***
Menace	L'utilisation effective du canal de vote électronique dépasse les limites de l'électorat autorisé (30% cantonal et 10% national)
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie
Conséquences	Si le résultat du vote avait pu changer en raison des votes de la part de l'électorat excédentaire, un recours pourrait conduire à l'annulation du scrutin dans un canton. La réputation des autorités serait moyennement affectée. Les essais de vote électronique pourraient être suspendus.

Évaluation

	Initiale		**Après mitigation**	
Probabilité	Basse		Basse	
Critères	**Valeur**	**Score**	**Valeur**	**Score**
Réputation et confiance	Moyen (2)	10	Moyen (2)	10
Légal	Haut (3)	15	Moyen (2)	10
Viabilité	Moyen (2)	6	Bas (1)	3
Finance	Moyen (2)	6	Bas (1)	3
Ressources	Moyen (2)	2	Bas (1)	1
Score d'impact		**39**		**27**