Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF
Section des droits politiques

Restructuration et reprise des essais

Rapport final du Comité de pilotage Vote électronique (CoPil VE)

30 novembre 2020

Table des matières

1. Rappel des faits ... 3

1.1 Le vote électronique en Suisse ... 3

1.2 Conditions générales régissant précédemment la phase d'essai ... 3
1.2.1 Tâches et rôles de la Confédération et des cantons ... 3
1.2.2 Introduction progressive en tant que troisième canal de vote ... 3
1.2.3 Contrôle et surveillance ... 3
1.2.4 Exigences de sécurité ... 4
1.2.5 Gestion des risques et des crises ... 4
1.2.6 Mesures de transparence ... 5

1.3 La situation en 2019 ... 5
1.3.1 Le système de La Poste Suisse ... 5
1.3.2 Le système du Canton de Genève ... 5
1.3.3 Mise en exploitation ... 6
1.3.4 Conclusions concernant la situation en 2019 ... 6

1.4 Situation fin 2020 ... 7

1.5 Restructuration de la phase d'essai ... 7
1.5.1 Mandat du Conseil fédéral et objectif ... 7
1.5.2 Collaboration entre la Confédération et les cantons ... 8

2. Dialogue avec les milieux scientifiques ... 9

2.1 Recours à des experts ... 9

2.2 Démarche retenue et modalités du dialogue ... 9

2.3 Synthèse des conclusions du dialogue ... 10
2.3.1 Evaluation générale ... 10
2.3.2 Mise à disposition d'un système sûr ... 10
2.3.3 Contrôle sur mandat et contrôle public ... 11

2.4 Évaluation du dialogue avec les milieux scientifiques ... 12

3. Description des mesures ... 13

A. Poursuite du développement des systèmes ... 13

B. Surveillance et contrôle efficaces ... 20

C. Renforcement de la transparence et de la confiance ... 28

D. Renforcement des liens avec les milieux scientifiques ... 35

4. Évaluation globale et marche à suivre ... 37

4.1 Résumé des orientations et échelonnement des mesures ... 37

4.2 Conséquences pour la Confédération et les cantons ... 38
4.2.1 Mesures en vue de la reprise des essais et des premières étapes après la reprise des essais ... 38
4.2.2 Développements de moyen à long terme ... 38
4.2.3 Sécurisation à long terme du financement ... 39

5. Conclusions ... 41

Annexe: Catalogue des mesures ... 42

1. Rappel des faits

1.1 Le vote électronique en Suisse

Le vote électronique en Suisse est en phase d'essai depuis 2004[1]. Le vote électronique est un maillon de la Stratégie suisse de cyberadministration de la Confédération et des cantons. Les bases légales sur lesquelles se fondent les essais sont l'art. 8*a* de la loi fédérale sur les droits politiques (LDP; RS 161.1), les art. 27*a* à 27*q* de l'ordonnance du 24 mai 1978 sur les droits politiques (ODP; RS 161.11) et l'ordonnance de la Chancellerie fédérale du 13 décembre 2013 sur le vote électronique (OVotE; RS 161.116). Le principe qui veut que « la sécurité prime la vitesse » est appliqué depuis que le projet a été lancé. En Suisse sont uniquement agréés les systèmes de vote électronique qui répondent aux sévères exigences de sécurité fédérales.

Depuis 2004, 15 cantons au total ont créé les bases légales nécessaires à l'utilisation du vote électronique, et ont proposé ce canal à une partie de leurs électeurs dans le cadre de plus de 300 essais réussis. Tous ont ouvert les essais aux électeurs suisses de l'étranger, et certains d'entre eux ont étendu cette participation à une partie des électeurs résidant en Suisse. Au cours des dernières années, les cantons avaient le choix entre deux systèmes de vote électronique : d'une part, le système du Canton de Genève, et d'autre part, celui de La Poste Suisse. Ces fournisseurs ayant tous deux retiré à la mi-2019 leur système de vote, le vote électronique n'est plus possible en Suisse actuellement (voir ch. 1.3.1 et 1.3.2).

1.2 Conditions générales régissant précédemment la phase d'essai

1.2.1 Tâches et rôles de la Confédération et des cantons

L'exercice des droits politiques se fait en fonction d'une répartition fédéraliste des compétences. Pour les scrutins fédéraux, les conditions générales sont fixées au niveau de la Confédération, et l'exécution des scrutins incombe aux cantons. Cette répartition des compétences, qui s'applique aussi au vote électronique, figure dans les bases légales régissant les essais de vote électronique. Ce sont ainsi les cantons qui décident s'ils veulent proposer le vote électronique à leurs électeurs dans le cadre d'un essai. Ils peuvent à cet égard exploiter leur propre système ou le système d'un autre canton ou d'une entreprise privée (art. 27*k*^{bis}, al. 1, let. b, ODP). La Confédération octroie les autorisations générales et les agréments pour les essais, aide les cantons sur les plans juridique, organisationnel et technique, et coordonne les projets au niveau national.

1.2.2 Introduction progressive en tant que troisième canal de vote

Le principe qui veut que « la sécurité prime le vitesse » prévaut depuis le début du projet. Le vote électronique doit ainsi être mis en place progressivement. Le droit fédéral soumet les systèmes de vote électronique et leur exploitation à des exigences de sécurité sévères. Celles-ci sont structurellement liées au développement progressif du vote électronique. Cette approche échelonnée prévoit une limitation du nombre des électeurs autorisés à voter par voie électronique, soit 30, 50 ou 100% de l'électorat cantonal et 10, 30 ou 100% de l'électorat national. Les électeurs suisses de l'étranger ne sont pas pris en compte dans la fixation de ces plafonds.

1.2.3 Contrôle et surveillance

<u>Procédure d'autorisation</u>

Les cantons qui souhaitent proposer le vote électronique doivent disposer d'une autorisation générale du Conseil fédéral et, pour chaque scrutin, d'un agrément de la ChF. Celle-ci s'assure dans le cadre de la procédure d'autorisation du respect des bases légales pertinentes.

Pour les cantons qui organisent pour la première fois des essais de vote électronique, l'autorisation générale est accordée pour cinq scrutins au maximum (art. 27*a*, al. 2, ODP). Le Conseil fédéral peut ensuite accorder une autorisation générale pour une durée plus longue (art. 27*a*, al. 3, ODP). Cette durée est de

[1] Les premiers essais de vote électronique ont été menés dès 2003 par le Canton de Genève (au niveau cantonal).

deux ans au maximum dans la pratique (FF 2013 4633). Enfin, le recours au vote électronique pour l'élection du Conseil national requiert pour chaque scrutin une autorisation générale spéciale (art. 27*a*, al. 4, ODP).

Contrôle indépendant

L'art. 7 OVotE dispose que les cantons veillent à ce que le respect des conditions soit assuré par des services indépendants. Si un canton souhaite proposer le vote électronique à plus de 30% ou 50% de son électorat, le contrôle du système devra répondre à des exigences plus sévères. Ces contrôles doivent en règle général être effectués par des services accrédités par le Service d'accréditation suisse (SAS). Les modalités de la certification sont arrêtées dans l'ODP et l'OVotE.

La ChF a en outre mis en place dans le cadre de la procédure d'autorisation des groupes dits « d'accompagnement », composés de représentants des cantons. Ces groupes ont effectué des tests utilisateurs, demandé des éclaircissements sur des dossiers de demande et favorisé l'échange d'informations.

1.2.4 Exigences de sécurité

Les exigences techniques et organisationnelles sont définies dans l'OVotE et dans son annexe. Les principales exigences qui doivent permettre le respect des normes de sécurité élevées qui s'appliquent en matière de vote électronique sont les suivantes :

- Vérifiabilité : la vérifiabilité permet de déceler les manipulations sans porter atteinte au secret du vote. L'OVotE distingue entre vérifiabilité individuelle et vérifiabilité complète :
  - La vérifiabilité individuelle permet au votant de déterminer si son suffrage a été enregistré correctement par le système, c'est-à-dire tel qu'il l'a exprimé. Le votant peut ainsi s'assurer que son suffrage n'a pas été modifié de façon abusive sur la plateforme de vote ou sur Internet.
  - La vérifiabilité complète garantit que les dysfonctionnements systématiques dans tout le processus de vote ou d'élection à la suite d'erreurs logicielles, d'erreurs humaines ou de tentatives de manipulation seront identifiés grâce à des moyens indépendants. Dans le souci de protéger le secret du vote, on fait en sorte que les suffrages ne se trouvent jamais sous une forme non chiffrée et qu'ils ne puissent pas être décryptés entre le moment où le vote intervient et le déchiffrement des suffrages mélangés selon un procédé cryptographique. Pour dissiper la contradiction apparente entre la transparence et le maintien du secret du vote, il faut recourir à des procédés cryptographiques conçus spécialement pour le vote électronique.
- Distribution des responsabilités : tout système de vote électronique repose sur un grand nombre d'ordinateurs configurés différemment, dont certains ne sont pas raccordés à Internet. Il s'agit également de prendre toutes mesures techniques et organisationnelles permettant de s'assurer que nul n'ait accès à des données critiques ou aux suffrages sans contrôle d'un ou plusieurs tiers.
- Contrôle : les systèmes sont contrôlés régulièrement par des organismes indépendants (audits externes, certification, audits de renouvellement pour la recertification). Le protocole cryptographique est vérifié par des spécialistes.
- Meilleures pratiques : le processus obligatoire d'amélioration continue prévoit que les systèmes sont adaptés systématiquement à l'état de la technique et protégés contre toute nouvelle faille de sécurité.

1.2.5 Gestion des risques et des crises

Le canton est responsable de l'exécution des scrutins fédéraux et assume les risques liés à l'utilisation du vote électronique. Il doit démontrer au moyen d'une appréciation des risques que tous les risques pour la sécurité se situent à un niveau suffisamment bas. Les exigences applicables à l'appréciation des risques sont définies à l'art. 3 en rel. avec l'art. 6 OVotE.

La Confédération et les cantons arrêtent dans une convention de crise les modalités à suivre en matière d'information, de collaboration et de communication en cas d'incident affectant le vote électronique.

1.2.6 Mesures de transparence

Il est primordial que les électeurs aient confiance dans les canaux de vote. C'est pourquoi différentes mesures de transparence ont-elles été prévues en matière de vote électronique. Le droit fédéral prescrit notamment l'obligation de publier le code source et la documentation technique pour les systèmes offrant la vérifiabilité complète (art. 7*a* et 7*b* OVotE). La Confédération et les cantons ont convenu en 2017 dans une déclaration d'intention que la première utilisation d'un système de vote électronique à vérifiabilité complète devrait être précédée d'un test public d'intrusion (PIT), dans le cadre duquel les personnes intéressées pourront lancer des attaques contre le système en vue de tester sa sécurité.

1.3 La situation en 2019

1.3.1 Le système de La Poste Suisse

La Poste propose depuis 2016 un système de vote électronique à vérifiabilité individuelle, qui a été mis en place par plusieurs cantons. Elle a également développé un nouveau système à vérifiabilité complète dont elle a publié le code source en février 2019. Ce système a en outre été soumis du 25 février au 24 mars 2019 à un test public d'intrusion (PIT) organisé par la Confédération, les cantons et La Poste Suisse. Les réactions des participants ont fourni des indications sur les moyens d'améliorer le respect de certaines des meilleures pratiques en matière de sécurité. Le PIT n'a permis de détecter ni intrusion dans l'infrastructure, ni manipulation des votes, ni violation du secret de vote[2].

Des failles majeures ont cependant été découvertes dans le code source publié, touchant la sécurité et la vérifiabilité. L'une de ces failles concernait la vérifiabilité individuelle et donc le système de La Poste qui était utilisé jusqu'à cette date. Ce constat a amené la ChF à demander un examen indépendant du système à vérifiabilité individuelle de La Poste Suisse, au terme duquel les processus opérationnels de La Poste Suisse ont été jugés positifs, mais qui a également révélé que le système comportait des failles qui n'avaient pas encore été identifiées[3].

La Poste a annoncé en juillet 2019 que le système à vérifiabilité individuelle ne serait plus utilisé et qu'elle se concentrerait sur le développement du système à vérifiabilité complète.

1.3.2 Le système du Canton de Genève

Le Canton de Genève fait partie des cantons pilotes qui ont proposé dès 2004 à leurs électeurs le vote électronique pour les scrutins fédéraux. Le Canton de Genève a développé et exploité à cette fin son propre système, le système CHVote. Plusieurs autres cantons ont eux aussi utilisé ce système, qui offrait la vérifiabilité individuelle. Le Canton de Genève travaille depuis 2016 au développement d'un système à vérifiabilité complète.

Le Canton de Genève a annoncé en novembre 2018 qu'il renonçait à développer son système CHVote, considérant qu'il n'avait pas à développer, exploiter et financer seul un système informatique d'une telle complexité et d'une telle ampleur[4]. Il a annoncé par ailleurs en juin 2019 qu'en raison de son report à la mi-août, la décision du Conseil fédéral d'autoriser ou non le recours au vote électronique pour l'élection du Conseil national interviendrait trop tardivement et qu'il mettrait fin à l'exploitation de son système avec effet immédiat[5]. Le système genevois aura donc été utilisé pour la dernière fois lors du scrutin du 19 mai 2019.

---

[2] Voir le rapport final du comité de pilotage « Vote électronique – Test public d'intrusion 2019 » (août 2019), sous www.bk.admin.ch > Droits politiques > Vote électronique > Test public d'intrusion.

[3] Plusieurs membres du groupe Vote électronique de la Haute école spécialisée bernoise (BFH) ont étudié la mise en œuvre du protocole cryptographique dans la spécification du système et dans le code source, et les chercheurs Olivier Pereira (Université de Louvain) und Vanessa Teague (Université de Melbourne) ont examiné la mise en œuvre du protocole sur la base de la spécification du système. L'entreprise Oneconsult a par ailleurs contrôlé la mise en œuvre des mesures de sécurité techniques et organisationnelles en se fondant sur les évaluations des risques des cantons. Les rapports sont publiés sur le site Internet de la ChF, sous www.bk.admin.ch > Droits politiques > Vote électronique > Rapports et études.

[4] Communiqué de presse du Canton de Genève du 28 novembre 2018, consultable sur www.ge.ch/document/point-presse-du-conseil-etat-du-28-novembre-2018#extrait-12897.

[5] Communiqué de presse du Canton de Genève du 19 juin 2019, consultable sur www.ge.ch/document/point-presse-du-conseil-etat-du-19-juin-2019.

Le Canton de Genève a publié en 2016 en *open source* plusieurs parties du code source de son système à vérifiabilité individuelle. Il a également publié en 2019 dans l'état de son développement le code source de son système à vérifiabilité complète.

1.3.3 Mise en exploitation

Le Conseil fédéral a décidé le 19 décembre 2018 d'ouvrir la procédure de consultation relative à la mise en exploitation du canal de vote électronique. La révision partielle proposée de la LDP aurait ainsi mis fin à la phase d'essai et fait du vote électronique le troisième canal de vote. Les principaux éléments du projet auraient été réglés dans la loi, notamment la vérifiabilité du vote et de l'établissement des résultats, la publicité des informations touchant le système utilisé et son fonctionnement, l'accessibilité aux électeurs handicapés et l'obligation pour les cantons de disposer d'une autorisation délivrée par la Confédération. Les cantons auraient conservé par ailleurs toute liberté de proposer ou non le vote électronique.

La consultation a montré qu'une majorité significative des cantons et des partis étaient favorables à l'instauration du vote électronique. La Conférence des gouvernements cantonaux et 19 cantons ont même approuvé le passage à la mise en exploitation. Les partis qui étaient a priori favorables au vote électronique ont toutefois estimé que le temps n'était pas encore venu de franchir ce pas. Aussi le Conseil fédéral a-t-il décidé le 26 juin 2019 de renoncer dans un premier temps à la révision partielle de la LDP[6].

1.3.4 Conclusions concernant la situation en 2019

De la mise en œuvre des mesures de transparence en 2019 et plus particulièrement de la découverte consécutive de failles de sécurité majeures dans les systèmes actuel et futur de La Poste, on peut tirer les conclusions suivantes :

- Les mesures de transparence mises en œuvre ont contribué significativement à l'amélioration des systèmes de vote électronique grâce aux connaissances qu'elles ont permis d'acquérir et aux failles qu'elles ont permis de découvrir.
- La publication du code source et le PIT ont permis d'acquérir de l'expérience dans les domaines du « contrôle public » et du recours à un nombre important d'experts externes. Elles ont également révélé qu'il y avait lieu d'agir sur la qualité du code source et sur les modalités de sa publication.
- La découverte de failles importantes a mis au jour des insuffisances graves dans le processus de développement mené précédemment et a mis en évidence la nécessité d'agir dans le domaine de l'assurance qualité.
- Les processus de contrôle et de certification précédemment mis en œuvre n'ont pas permis de détecter les failles et insuffisances identifiées par la suite. Les processus actuels n'ont pas été suffisamment efficaces.

Le projet de vote électronique et ses développements ont donné lieu au dépôt d'interventions parlementaires aux niveaux tant fédéral que cantonal. Les unes concernent les exigences à remplir par les fournisseurs de systèmes[7], les autres remettent en question la sécurité en général du vote électronique ou demandent que la poursuite de la phase d'essai soit soumise à certaines conditions[8]. Le débat sur le vote électronique est également marqué par des spéculations sur la possible ingérence de pays tiers dans les élections et par différents incidents touchant la cybersécurité et la protection des données qui ont été

[6] Communiqué de presse du Conseil fédéral du 27 juin 2019, consultable sur www.bk.admin.ch > Droits politiques > Vote électronique > Communiqués de presse.

[7] Confédération : Mo. 18.4225 Wehrli « Vote électronique dans le mandat de la poste »; Mo. 18.4375 Sommaruga « Vote électronique. Pour un engagement rapide et fort en faveur d'un système en main publique et en "open source" » ; cantons : adoption notamment d'un projet de loi par le Grand Conseil genevois prévoyant que le système de vote électronique utilisé par le Canton doit être, dans sa conception, sa gestion et son exploitation, entièrement contrôlé par des collectivités publiques.

[8] Confédération : Iv. pa. Müller 18.427 « Oui au vote électronique, mais la sécurité doit primer »; Iv. pa. Zanetti 18.468 « Vote électronique. Suspendre les travaux »; Mo. 19.3294 Zanetti « Remplacer le vote électronique par l'envoi électronique »; cantons : voir notamment le Grand Conseil du Canton de St-Gall, qui a rejeté la motion 42.19.07, qui demandait l'interruption immédiate des essais de vote électronique, et le Grand Conseil du Canton de Lucerne, qui a rejeté la motion 683, qui demandait que le vote électronique fasse l'objet d'un moratoire dans le canton de Lucerne.

rapportés, qu'ils aient ou non un lien direct avec le vote électronique. Le vote électronique s'inscrit ainsi dans un débat de fond sur les opportunités et les risques du tournant numérique[9].

1.4 Situation fin 2020

Les développements de ces dernières années ont également entraîné des changements dans la situation du marché, tant du côté de l'offre que de la demande. Parmi les fournisseurs de systèmes, seule la Poste Suisse demeure actuellement. Elle est le seul fournisseur à investir dans le développement d'un système de vote électronique. L'objectif d'une stratégie multiproduits, formulée par la Confédération et les cantons en 2017, n'a pas été atteint comme souhaité. Du système de vote électronique du canton de Genève, reste le noyau comportant la vérifiabilité complète qui a été achevé par la Haute école spécialisée de Berne et publié sous licence open source. Il a été démontré que le développement et l'exploitation d'un système avec vérifiabilité complète est une entreprise exigeante et complexe. On peut donc supposer que la situation ne changera pas très prochainement.

La situation du côté de la demande a également considérablement changé. Si des essais de vote électronique ont été menés dans 14 cantons lors de la votation du 14 juin 2015, dix cantons proposaient encore le canal de vote électronique lors de la votation du 10 février 2019. À l'heure actuelle, seuls quelques cantons s'efforcent de reprendre rapidement les essais. Les autres cantons ont d'autres projets de numérisation. Cela a pour conséquence que les responsables du vote électronique dans les cantons, dont certains sont chargés du vote électronique depuis de nombreuses années, assument d'autres tâches et que le savoir-faire se perd. La réussite de la restructuration du vote électronique dépend essentiellement de la volonté du fournisseur de système et des cantons restants de continuer à investir dans le développement du système de la Poste et dans la reprise des essais, et de l'adhésion de nouveaux cantons au cours des prochaines années.

1.5 Restructuration de la phase d'essai

1.5.1 Mandat du Conseil fédéral et objectif

Le Conseil fédéral a chargé en juin 2019 la ChF de concevoir avant la fin 2020 avec les cantons une restructuration de la phase d'essai du vote électronique[10]. Il a pris cette décision au vu et des résultats de la consultation qui avait été organisée en vue d'une mise en exploitation du vote électronique et des failles de sécurité qui avaient été découvertes dans le système de La Poste.

Conformément au mandat du Conseil fédéral, la restructuration de la phase d'essai devait s'articuler autour des objectifs suivants :

1. poursuite du développement des systèmes
2. surveillance et contrôles efficaces
3. renforcement de la transparence et de la confiance
4. renforcement des liens avec les milieux scientifiques

Toujours conformément au mandat du Conseil fédéral, il s'agira de vérifier dans le cadre de cette restructuration dans quelle mesure devront être revues les exigences prévues par le droit fédéral. Celles-ci devront permettre d'évaluer et de garantir de manière effective la qualité et la sécurité des systèmes. Elles devront au surplus répondre aux attentes des décideurs politiques et du public en matière de sécurité et de transparence, de façon à permettre de renforcer la confiance dans ces systèmes.

[9] Voir notamment l'institut de recherche Sotomo (2018): « Digitale Lebensvermessung und Solidarität, Verhalten und Einstellungen der Schweizer Bevölkerung », Zurich; Digitalswitzerland (2019): « Am digitalen Puls der Bevölkerung, Ein Bericht über die Einstellung der Bevölkerung zum Thema Digitalisierung, aufgenommen im Rahmen des Digitaltags 2019 ».

[10] Communiqué de presse du Conseil fédéral du 27 juin 2019, consultable sur www.bk.admin.ch > Droits politiques > Vote électronique > Communiqués de presse.

1.5.2 Collaboration entre la Confédération et les cantons

Suite au mandat du Conseil fédéral, le comité de pilotage Vote électronique (CoPil VE) a mis en place le 29 novembre 2019 le sous-groupe de travail Restructuration et reprise des essais (SGTRR), en le chargeant de définir des mesures en vue de la restructuration et de la reprise des essais. Il devra également proposer un échelonnement des mesures permettant de reprendre les essais avec le système à vérifiabilité complète de La Poste dans le cadre de la première étape de la restructuration.

Le SGTRR était composé de l'équipe du projet Vote électronique de la ChF (direction et secrétariat) et de représentants des cantons de Berne, Fribourg, Bâle-Ville, Saint-Gall, Grisons, Argovie, Thurgovie et Neuchâtel. Le SGTRR s'est réuni entre décembre 2019 et octobre 2020. La Poste, en sa qualité de dernier fournisseur de système en lice, était présente à ces réunions[11]. Le présent rapport inclut les résultats des travaux du SGTRR. Le CoPil VE a adopté le rapport lors de sa séance du 30 novembre 2020.

[11] En sa qualité de fournisseur, La Poste est responsable envers les cantons du développement et de l'exploitation de son système de vote électronique. Elle a été invitée à participer aux entretiens afin d'apporter son savoir-faire dans la mise en œuvre pratique des exigences de sécurité. Elle n'a pas participé aux décisions concernant les mesures de restructuration.

2. Dialogue avec les milieux scientifiques

2.1 Recours à des experts

Pour établir les bases de la restructuration, la ChF, avec la participation des autres membres du SGTRR, a mené un dialogue avec des experts issus de la science et quelques experts issus de l'industrie. Les experts externes mandatés par la ChF comprenaient des représentants de l'informatique, de la cryptographie et des sciences politiques[12]. Ils ont assisté le SGTRR dans sa réflexion sur les actions à engager et les questions concernant les mesures éventuellement à prendre en vue de la restructuration. Le dialogue avec la communauté scientifique a été financé par des fonds en provenance de eGovernment Suisse.

Les représentants d'autres cantons[13] ou services fédéraux[14] ont été tenus informés en permanence de l'avancement du dialogue avec la science et ont eu accès à la plate-forme de discussion.

2.2 Démarche retenue et modalités du dialogue

En vue du dialogue avec les experts externes, la ChF a défini de concert avec les autres membres du SGTRR les blocs thématiques suivants, dans le cadre desquels différentes questions ont été débattues :

1. Risques et mesures d'aujourd'hui et de demain ;
2. Analyses indépendantes ;
3. Collaboration avec les milieux scientifiques et inclusion du grand public ;
4. Transparence et renforcement de la confiance ;
5. Analyse de risques et plan d'action ;
6. Gestion des crises.

Au début du dialogue, soit en février 2020, les experts ont reçu un questionnaire complet comportant une soixantaine de questions. En raison des mesures prises pour contenir le coronavirus, les ateliers initialement prévus ont été remplacés par un dialogue écrit et modéré sur une plate-forme Internet. Les discussions sur la plate-forme ont eu lieu entre mai et juillet 2020.

Le questionnaire couvrait les six blocs thématiques. Les experts ont pu exprimer des considérations générales sur le sujet du « vote électronique digne de confiance », répondre à des questions spécifiques en rapport avec les mesures possibles et proposer d'autres mesures. Le questionnaire devait permettre de fournir une vue d'ensemble permettant de dégager et de traiter de manière structurée aussi bien les points de consensus que ceux qui exigeaient encore d'être débattus et éclaircis.

Sur la base de l'évaluation des réponses faites au questionnaire, les blocs de discussion suivants ont été définis pour la plate-forme Internet :

Blocs thématiques	Blocs de discussion
1	Bloc 1 : Efficacité de la cryptographie
1	Bloc 2 : La diversité pour renforcer la sécurité et la confiance
1	Bloc 3 : Imprimerie (génération distribuée des paramètres)
1	Bloc 4 : Public Bulletin Board
2	Bloc 5 : Vérification commanditée
4	Bloc 6 : Développement et publication
4	Bloc 7 : Test public d'intrusion / Bug Bounty
5	Bloc 8 : Gestion des risques

[12] Voir la liste des experts de juin 2020 sur www.bk.admin.ch > Droits politiques > Vote électronique.

[13] Cantons de Zurich, de Lucerne, de Glaris, du Tessin et de Genève.

[14] Centre national pour la cybersécurité (NCSC), Base d'aide au commandement (BAC), Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité commune relative au cyberespace et OIC MELANI du Service de renseignement de la Confédération (SRC).

5	Bloc 9 : Audits de limitation des risques et contrôles de plausibilité pour mitiger les risques
6	Bloc 10 : « Forensic Readiness »
tous	Bloc 11 : Vue d'ensemble (« Big Picture »)
3	Bloc 12 : Dialogue futur

Pour chaque bloc de discussion, des thèses, des propositions de solutions et des questions ouvertes ont été préparées en vue d'une discussion écrite avec et entre les experts. Les participants ont discuté de divers sujets en parallèle, ont pu commenter les réponses des autres participants ou se poser des questions les uns aux autres. Les contributions étaient visibles par tous les participants. L'objectif était de dégager un consensus, de clarifier les questions ouvertes, de valider les conclusions et, le cas échéant, de constater les divergences.

Plus de 700 déclarations au total ont été enregistrées sur la plate-forme. Parmi elles, il y avait aussi bien des réponses courtes que des réponses détaillées. Parallèlement à la discussion sur la plate-forme, certains experts ont été chargés de traiter d'autres questions concernant les mesures possibles. A l'issue du dialogue, la ChF en a préparé une synthèse avec d'autres membres du SGTRR. Les documents concernés sont publiés sur le site Internet de la ChF[15].

Le dialogue avec les experts a été modéré à la demande de la ChF par Christian Folini, consultant senior en sécurité chez netnea AG.

2.3 Synthèse des conclusions du dialogue

2.3.1 Evaluation générale

Les experts estiment qu'il faut intervenir en ce qui concerne la sécurité, la transparence et le contrôle indépendant. Ils sont néanmoins d'avis que des progrès significatifs ont été accomplis au courant des 15 dernières années. Ils recommandent d'analyser également la sécurité des autres canaux de vote. Ils invitent en outre à approfondir la question de la création d'un climat de confiance.

Les experts soulignent l'importance d'associer en tout temps les spécialistes - en particulier des experts issus du monde scientifique - à la conception, au développement et au contrôle des systèmes de vote électronique. La création d'un comité scientifique a été évoquée à plusieurs reprises.

2.3.2 Mise à disposition d'un système sûr

Les prescriptions en matière de sécurité doivent rester la prérogative des autorités

Les experts estiment que l'appréciation des risques et le cas échéant la prescription de mesures doivent rester l'affaire des autorités. Un comité scientifique pourrait les assister dans ce domaine.

Standardisation des composants cryptographiques

Les preuves de sécurité dans le domaine de la cryptographie déjà exigées aujourd'hui sont cruciales. Il convient de les adapter constamment à l'état de la science et des connaissances. Les experts recommandent en outre aux autorités d'œuvrer à la standardisation des composants cryptographiques.

Garantir la qualité et la vérifiabilité du code source

Il faut veiller à ce que la documentation du système et le code source soient disponibles sous une forme qui permette un contrôle efficace de leur conformité avec les exigences légales. Les experts ont cité

[15] www.bk.admin.ch > Droits politiques > Vote électronique

plusieurs standards qui pourraient servir de base aux processus de développement. La simplicité doit être la règle maîtresse de la conception du système.

Plus de diversité comme condition fondamentale de la fiabilité

Les experts estiment que la diversité des composants importants pour la vérifiabilité (composants de contrôle et de vérification) est une condition fondamentale de la fiabilité d'un système. Grâce au fonctionnement correct d'autres composants, les erreurs dans certains composants ne devraient pas affecter la vérifiabilité (gain de sécurité exponentiel). Le logiciel fait partie des éléments à diversifier. Les experts voient également un potentiel d'amélioration dans la génération des paramètres système (par ex. des codes de contrôle pour la vérifiabilité individuelle), qui devrait être vérifiable et distribuée. Ils ont ébauché des solutions d'impression partagée des cartes de légitimation. Si les experts sont bien conscients du fait que la diversité augmente les coûts et la complexité de l'exploitation, ils soulignent néanmoins la plus-value qu'elle apporte.

Tableau d'affichage public au service de la vérifiabilité

La possibilité de recourir à un tableau d'affichage public (Public Bulletin Board) - instrument évoqué dans la littérature sur le vote électronique - afin de développer la vérifiabilité et d'améliorer son indépendance a été examinée. Les experts estiment qu'un tel instrument est susceptible de contribuer à la confiance mais relèvent que celle-ci pourrait être affectée en cas d'erreur de conception et de réalisation. Les besoins des votants, notamment en matière de communication, de présentation visuelle et de convivialité, doivent être établis et pris en compte suffisamment tôt.

2.3.3 Contrôle sur mandat et contrôle public

Contrôle sur mandat

La certification des systèmes n'est pas considérée comme déterminante. Une certification (selon la norme ISO27001) pourrait néanmoins s'avérer judicieuse dans le cadre du contrôle de l'exploitation. Les autorités devraient privilégier les contrôles indépendants effectués par des personnes dotées des compétences nécessaires plutôt que recourir à des certifications. Il faut faire appel à des cryptographes également pour le contrôle du code source et de l'exploitation. Le contrôle doit reposer sur un concept global afin d'éviter les lacunes. Il doit faire l'objet d'une commande de la Confédération ou d'un comité indépendant.

Contrôle public

Les experts attachent une grande importance au contrôle public. Ils préconisent donc de remplacer le test public d'intrusion mené en 2019 par un programme Bug Bounty permanent, donnant droit à une compensation financière. Le programme Bug Bounty ne doit pas se limiter à pirater l'infrastructure du fournisseur, mais viser à détecter les erreurs dans la documentation du système et le code source. Les objectifs, les modalités ainsi que la haute surveillance sur le programme Bug Bounty doivent être arrêtées par la Confédération ou un comité indépendant.

D'autres mesures, telles que des hackathons, visant à associer le public sont envisageables en plus du programme Bug Bounty. Il pourrait également être judicieux de faire appel à des personnes sans bagage technique, par ex. dans le cadre d'un projet de sciences participatives consacré à la convivialité.

Transparence et publication du code source

La transparence est la condition sine qua non d'un contrôle public efficace. Les experts estiment qu'il faut absolument renoncer à exiger une déclaration de confidentialité lors de la publication du code source.

Tous les documents nécessaires pour comprendre comment le système fonctionne et est exploité doivent être publiés avec le code source. Il doit en outre être possible aux participants de tester le système sur leur ordinateur. Si les adaptations du code source ne sont pas immédiatement publiées, les experts recommandent de procéder à une première itération des contrôles internes afin d'éviter des erreurs susceptibles de saper la confiance.

Il faut publier les failles et répondre aux remarques du public. Il appartient à la Confédération de préciser les modalités à cet égard. La plupart des experts recommandent en outre de publier les rapports de contrôle. Ils ont cependant été nombreux à signaler que des rapports de mauvaise qualité pourraient affecter la confiance.

Les experts sont d'avis qu'une publication même sans licence libre[16] permet de mener un contrôle public adéquat. Ils estiment néanmoins qu'une publication sous licence libre offre de meilleures garanties de succès.

Procédure en cas de non-conformités

Idéalement, le contrôle a lieu suffisamment tôt pour que les non-conformités puissent être découvertes et éliminées avant l'exploitation du système. Des processus décisionnels doivent être mis en place pour les non-conformités découvertes plus tard.

Il n'est pas nécessaire d'interrompre l'exploitation d'un système de vote électronique pour n'importe quelle non-conformité. Les experts estiment qu'il est raisonnable d'accepter des risques mineurs. Toute la difficulté réside dans l'appréciation correcte du risque. Il peut être utile de faire une comparaison avec des risques qui ont déjà été acceptés. Il faut également tenir compte du fait que sans le vote électronique les Suisses de l'étranger perdent de fait une partie de leur droit de vote et que renoncer à ce canal implique de recourir davantage au vote par correspondance, qui n'est pas non plus exempt de risque. Plus une non-conformité affecte le système et moins elle est circonscrite aux processus environnants, plus il est nécessaire de l'éliminer. En principe, les erreurs dans le protocole cryptographique ou dans sa mise en œuvre dans le code source ne doivent pas être acceptées.

2.4 Évaluation du dialogue avec les milieux scientifiques

La participation au dialogue d'experts issus de différents domaines a permis de mener un large débat sur la nécessité d'agir et sur les solutions possibles, et elle a fourni au SGTRR une bonne base de travail. Les réactions des experts à ce dialogue ont été positives, et ils se sont félicités d'y avoir été associés. Ils se déclarent même en faveur d'une poursuite de ce dialogue dans le cadre d'un échange permanent entre autorités et scientifiques. Si le dialogue qui a eu lieu s'est concentré plus particulièrement sur des questions d'ordre technique, il devrait mettre davantage l'accent à l'avenir sur des sujets à portée sociale. Les experts ont estimé par ailleurs que le débat autour de la sécurité devrait concerner non seulement le vote électronique, mais aussi les autres canaux de vote. Une vision globale des attaques possibles permettrait d'améliorer la sécurité des élections et des votations dans son ensemble.

La Confédération et les cantons sont d'avis qu'une collaboration renforcée devra également intervenir à l'avenir avec les experts de l'industrie et de la science. Aussi le SGTRR envisage-t-il des mesures destinées à promouvoir une telle participation dans plusieurs domaines.

[16] Les licences libres permettent d'utiliser un logiciel dans n'importe quel but.

3. Description des mesures

Les mesures pour la restructuration et la reprise des essais sont commentées et évaluées ci-après et un lien est établi avec le dialogue avec les milieux scientifiques (voir chapitre 2.3 et le résumé des résultats du dialogue).[17] Une vue d'ensemble des mesures est disponible dans le catalogue de mesures en annexe. Les contributions des experts seront prises en compte dans la mise en œuvre des mesures.

A. Poursuite du développement des systèmes

N°	Mesure	Calendrier mise en œuvre	Responsabilité
A.1	Précision des critères qualité pour le code source et la documentation y relative	Reprise des essais	Exigences : ChF Mise en œuvre : cantons et fournisseur du système

Objectif et description de la mesure

La qualité du code source et de la documentation est un élément central pour la sécurité du vote électronique. Les bases légales actuelles imposent plusieurs exigences y-relatives. Il s'agit toutefois plutôt de descriptions générales, telles que l'obligation de préparer et de documenter le code source conformément aux bonnes pratiques (art. 7*b* OVotE) et de mettre en œuvre certains éléments des *Common Criteria*, qui ont été sélectionnés sur la base du profil de protection de l'Office fédéral allemand pour la sécurité en matière de technologies de l'information (BSI). Aussi est-il nécessaire d'agir dans ce domaine. La ChF devra ainsi préciser les critères de qualité qui s'appliquent aujourd'hui au code source et à sa documentation. Des critères clairs devront garantir une qualité élevée des systèmes de vote électronique. En outre, les audits de tous les acteurs et du public devront être facilités.

Pour préciser les critères de qualité, la ChF s'inspirera de normes existantes (par ex. *ISO Systems and software Quality Requirements and Evaluation*) et elle adaptera en conséquence les bases légales. Ces critères devront être respectés lorsque les essais reprendront. Enfin, les processus d'assurance qualité liés au développement des logiciels s'appuieront eux aussi sur ces critères.

Dialogue avec les milieux scientifiques

Le code source et la documentation devront être de grande qualité et se présenter sous une forme permettant un contrôle efficace de la conformité avec les exigences légales et avec le modèle de sécurité. En outre, la simplicité devra présider à la conception des systèmes. La qualité du code source et de la documentation étant une question transversale, on se référera aux commentaires concernant les autres mesures pour des évaluations plus détaillées de la part des experts (par ex. contrôles indépendants, assurance qualité tout au long du processus de développement, publication du code source).

Impact de la mesure[18] et appréciation globale du CoPil VE

Une qualité élevée du code source et de la documentation a toujours été requise pour le vote électronique. Il s'agit maintenant de préciser les exigences de qualité correspondantes, ce qui permettra d'une part d'apporter aux fournisseurs de systèmes de la transparence en ce qui concerne le niveau d'exigences requis et, d'autre part, d'aider à garantir que le logiciel sera développé dans le respect de la qualité attendue. Cela permettra en outre d'améliorer la vérifiabilité du code source et de la documentation. Cette mesure est liée à l'assurance qualité dans le processus de développement (mesure A.2), à la construction et au déploiement (mesure A.3), aux audits indépendants (mesures B.1 et B.2) et à la publication du code source (mesure C.2).

Garantir une qualité élevée du code source et de la documentation entraîne généralement des coûts élevés. Mais comme cette mesure constitue une spécification des critères de qualité, elle ne devrait pas occasionner de coûts supplémentaires pour la Confédération et les cantons.

[17] Les documents sont publiés in extenso sur le site de la ChF, sous www.bk.admin.ch > Droits politiques, Vote électronique.

[18] S'agissant des conséquences financières, il est indiqué à chaque fois une estimation des coûts supplémentaires à supporter par la Confédération et les cantons (coûts externes ou ressources supplémentaires). Échelle : bas (<50'000 CHF) / moyen (50'000-500'000 CHF) / élevé (500'000-1 million CHF) / très élevé (> 1 million CHF).

N°	Mesure	Calendrier mise en œuvre	Responsabilité
A.2	Renforcement de l'assurance qualité dans le processus de développement du système	Reprise des essais	Exigences : ChF Mise en œuvre : cantons, fournisseur du système

Objectif et description de la mesure

La qualité des systèmes de vote électronique doit être garantie tout au long du processus de développement. Afin de renforcer l'assurance qualité, les exigences de la ChF seront précisées. Il s'agit d'atteindre les objectifs suivants :

- Les modifications apportées au système doivent pouvoir être traçables et contrôlées.
- La traçabilité entre les différents éléments de la documentation (protocole, spécification, architecture, etc.) et le code source doit pouvoir être assurée de manière continue et dans les deux sens.
- Les résultats des processus de revue sont intégrés dans le développement.
- La conformité aux exigences légales est garantie et maintenue tout au long du cycle de vie.

La ChF précisera les exigences correspondantes dans les bases légales en vue de la reprise des essais.

Dialogue avec les milieux scientifiques

Les experts ont mentionné différentes normes susceptibles de constituer une base possible pour les processus de développement. De nombreux experts mettent en avant à cet égard la traçabilité du processus de développement. Mais ils ont également souligné l'importance de la transparence, du recours à des experts indépendants et de la mise à disposition correcte du système à partir du code source (voir les mesures A.1, A.3 et C.2). Les preuves de sécurité déjà exigées aujourd'hui en matière de cryptographie sont importantes, et devront être adaptées en continu à l'état actuel de la science. Les experts conseillent également aux autorités de travailler à la standardisation des composants cryptographiques.

Impact de la mesure et appréciation globale du CoPil VE

Il est important de renforcer l'assurance qualité dans le processus de développement. La spécification des exigences actuelles permettra de s'assurer que la qualité du système sera prioritaire tout au long du processus de développement. Cela devrait garantir un niveau élevé de sécurité du système et faciliter les contrôles aux autorités et aux experts indépendants. Cette mesure ne devrait avoir aucune incidence financière directe pour la Confédération et les cantons.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
A.3	Mise en œuvre d'une méthode éprouvée et vérifiable de construction et de déploiement	Reprise des essais	Exigences : ChF Mise en œuvre : cantons, fournisseur du système

Objectif et description de la mesure

Il s'agit de garantir une mise à disposition correcte du système depuis le code source jusqu'à son installation en production (construction et déploiement). Il incombe à cet égard au fournisseur du système d'utiliser une méthode de construction et de déploiement à la fois éprouvée et traçable. Les exigences pertinentes en matière de construction et de déploiement seront revues pour atteindre les objectifs suivants :

- La méthode de construction et de déploiement permet de s'assurer que le logiciel utilisé est conforme à la version publiée, testée et autorisée.
- En plus de cette traçabilité, la méthode de construction et de déploiement doit empêcher autant que possible toute manipulation des composants du système.
- Il faut éviter que les outils de développement et librairies utilisés n'introduisent des vulnérabilités pertinentes pour le logiciel qui rendraient le système vulnérable aux attaques. Il est mis en place un processus de traitement des non-conformités (voir mesure B.3).

La ChF adaptera les bases légales pertinentes afin d'imposer les exigences correspondantes aux fournisseurs de systèmes. Ces nouvelles exigences devront être remplies avant toute reprise des essais.

Dialogue avec les milieux scientifiques

Les experts ont confirmé l'importance d'utiliser une méthode de construction et de déploiement efficace et vérifiable. Cette méthode doit être adaptée à la fourniture de systèmes sécurisés et permettre la traçabilité et le contrôle du logiciel utilisé. Les experts ont par ailleurs fait des recommandations pour les bonnes pratiques en matière de construction et de déploiement.

Impact de la mesure et appréciation globale du CoPil VE

Cette mesure, avec les mesures A.1 et A.2, permettra d'améliorer la qualité, la traçabilité et la vérifiabilité du système tout au long du processus. La mise en œuvre de cette mesure n'aura pas d'impact financier pour la Confédération ; quant à l'impact financier pour les cantons, il est jugé faible.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
A.4	Utilisation de composants indépendants du fournisseur (« Verifier », composants contrôle)	Etude et proposition composants de contrôle en ligne au CoPil VE : jusqu'à 2 ans après la reprise des essais Mise en œuvre sous réserve : environ 5 ans après la reprise des essais	Etude composants de contrôle en ligne : cantons, avec la participation de la ChF

Objectif et description de la mesure

Il est possible de renforcer la vérifiabilité en veillant à une diversité et à une indépendance accrue des logiciels de différents composants. Les composants suivants pourraient être exploités avec un logiciel ne provenant pas du fournisseur du reste du système :

- Composants de contrôle permettant la génération des codes de vérification et la conservation des suffrages jusqu'au dépouillement (ou « composants de contrôle en ligne »).
- Composants de contrôle pour le mélange des votes.
- Verifier permettant de s'assurer que tous les suffrages enregistrés par les composants de contrôle en ligne ont été correctement mélangés, dépouillés et décomptés.

Le CoPil VE a l'intention d'utiliser des composants de contrôle en ligne indépendants du fournisseur dans un délai d'environ cinq ans après la reprise des essais. Cette déclaration d'intention est subordonnée à l'obtention d'un financement. Une masse critique de cantons actifs est nécessaire pour répartir les charges. En particulier, un nombre suffisant de cantons doit être disposé à supporter les coûts à la charge des cantons. Il en va de même avec la réserve qu'aucune raison importante inconnue à ce jour ne s'oppose à une mise en œuvre ultérieure. La priorité sera accordée à cet égard au développement des informations de base dans le domaine des composants de contrôle en ligne. Dans un premier temps, une étude sera réalisée en vue de revoir le cas échéant les compétences en matière d'attribution des contrats, de maintenance, d'exploitation et de traitement des questions techniques qui pourraient se poser. Il s'agira notamment de montrer les conséquences sur les processus opérationnels au niveau cantonal et les coûts de mise en œuvre. L'étude devra en outre présenter une planification concrète possible pour la mise en œuvre (qui, selon une première évaluation des cantons, devrait prendre trois à cinq ans au moins). C'est sur la base de cette étude que sera prise la décision de mise en œuvre. La préparation de l'étude relèvera de la responsabilité des cantons.

Une fois l'étude terminée, la ChF et les cantons soumettront au CoPil VE une proposition de marche à suivre.

Dialogue avec les milieux scientifiques

La diversité des composants qui jouent un rôle important pour la vérifiabilité (composants de contrôle et *verifier*) est selon les experts une condition essentielle de la fiabilité des systèmes de vote électronique : les erreurs affectant certains composants ne devraient pas avoir d'impact négatif sur la vérifiabilité grâce à d'autres composants fonctionnant correctement (gain de sécurité exponentiel). Aussi les experts préconisent-ils l'installation de logiciels indépendants des fournisseurs sur les principaux composants (« composants de contrôle » et *verifier*). Ils admettent qu'une plus grande diversité se traduira par des coûts élevés et par une exploitation plus complexe, mais soulignent la plus-value qui en résultera.

Impact de la mesure et appréciation globale du CoPil VE

La fiabilité d'un système de vote électronique dépend notamment de la diversité des éléments qui jouent un rôle important pour la vérifiabilité. C'est pourquoi l'utilisation de composants de contrôle en ligne indépendants est considérée à moyen terme.

L'établissement de l'étude aura un impact financier faible à moyen pour les cantons, et aucun pour la Confédération. La conception et la mise en œuvre concrètes de composants de contrôle indépendants et les coûts induits devront être examinés plus en détail dans le cadre de l'étude. S'appuyant sur les hypothèses actuellement formulées pour la conception, une première estimation de La Poste indique que la mise en œuvre des composants de contrôle indépendants (exploité par La Poste) entraînerait les coûts suivants :

- Coûts uniques : de 1,8 à 2,2 millions de francs
- Coûts récurrents (en moyenne) : de 0,6 à 0,8 francs par an

La Haute école spécialisée de Berne (BFH) a estimé que la mise en place d'un *verifier* indépendant aurait les incidences financières suivantes :

- Coûts uniques : de 900 000 à 1 million de francs
- Coûts récurrents (en moyenne) : 200 000 francs par an

Compte tenu de la répartition actuelle des compétences, ces coûts devraient être supportés par les cantons. Ceux-ci soulignent toutefois que les coûts de mise en œuvre excéderaient les ressources dont ils disposent. Il s'agira donc d'envisager un cofinancement par la Confédération.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
A.5	Réduction des hypothèses de confiance dans le processus d'impression et le logiciel qui génère les paramètres cryptographiques	Approfondissement et adaptation du protocole cryptographique : 1 an après la reprise des essais Proposition au CoPil VE : jusqu'à 2 ans après la reprise des essais Mise en œuvre sous réserve : environ 4 ans après la reprise des essais	Clarification des questions ouvertes concernant les exigences : ChF Mise en œuvre : cantons

Objectif et description de la mesure

La vérifiabilité du vote électronique ne fonctionne que si les paramètres cryptographiques pertinents sont correctement générés lors de la phase de préparation et que les valeurs confidentielles (comme les codes de vérification) ne tombent pas entre de mauvaises mains. Les bases légales actuelles permettent de faire imprimer les valeurs confidentielles des électeurs par une presse unique. Les mesures de sécurité organisationnelles doivent donc être suffisamment étendues pour garantir que ces valeurs resteront confidentielles. Il n'est pas précisé dans quelle mesure le choix correct des paramètres pourrait lui aussi reposer sur des mesures organisationnelles. Il est donc nécessaire d'agir pour renforcer l'efficacité de la vérifiabilité.

Il est prévu de réduire les hypothèses de confiance admissibles dans le processus d'impression et le logiciel qui génère les paramètres cryptographiques. On s'assurera au moyen d'un logiciel indépendant du fournisseur que les paramètres cryptographiques et en particulier les codes de vérification ont été générés de manière aléatoire. Pour atteindre l'entropie souhaitée, quatre composants de contrôle au moins doivent être utilisés pour la génération de valeurs privées. Dans une évaluation par échantillonnage, il s'agira de vérifier des cartes de vote prises au hasard afin de s'assurer que les valeurs imprimées correspondent bien aux valeurs vérifiées.

Le CoPil VE a l'intention d'adapter la génération des paramètres ainsi que le processus d'impression dans un délai d'environ quatre ans après la reprise des essais. Cette déclaration d'intention est subordonnée à l'obtention d'un financement. Une masse critique de cantons actifs est nécessaire pour répartir

les charges. En particulier, un nombre suffisant de cantons doit être disposé à supporter les coûts à la charge des cantons. Il en va de même avec la réserve qu'aucune raison importante inconnue à ce jour ne s'oppose à une mise en œuvre ultérieure.

Dans un premier temps, la ChF et les cantons approfondiront la solution envisagée, et les cantons feront procéder à l'adaptation du protocole cryptographique. Ils définiront leurs processus en collaboration avec La Poste. Une première estimation du calendrier a montré que la mise en œuvre (y compris l'adaptation du protocole cryptographique) prendrait certainement trois ans. La planification de la mise en œuvre devra être approfondie dans le cadre de la première étape.

Une fois achevés les travaux d'approfondissement, la ChF et les cantons soumettront au CoPil VE une proposition détaillée de mise en œuvre.

Dialogue avec les milieux scientifiques

Les experts sont d'accord pour considérer que la génération correcte des paramètres (comme les codes de vérification pour la vérifiabilité individuelle) doit être vérifiable et, si nécessaire, répartie (sur la base de plusieurs valeurs aléatoires). Ils voient dans ce domaine un potentiel d'amélioration. S'agissant de l'impression des cartes de vote, ils ont esquissé des solutions pour un processus d'impression distribué. Ils suggèrent ainsi que l'impression des valeurs se fasse non pas avec la même presse, mais qu'elle soit répartie sur plusieurs. Les experts admettent qu'une plus grande diversité se traduira par des coûts élevés et par une exploitation plus complexe, mais soulignent la plus-value qui en résultera.

Impact de la mesure et appréciation globale du CoPil VE

Dans le cadre du dialogue avec les milieux scientifiques, la ChF, en collaboration avec les cantons, a soumis aux experts les grandes lignes d'une éventuelle réglementation dans ce domaine. Cette mesure apporterait un gain en termes de sécurité, mais elle prévoit toujours l'utilisation d'une seule presse à imprimer, pour des raisons de coût. La Poste et la Haute école spécialisée de Berne (BFH) ont réalisé pour leurs systèmes respectifs une première étude sur la faisabilité des exigences prévues par la réglementation proposée, et l'ont soumise à plusieurs experts. Les résultats montrent que les exigences semblent être réalisables. La Poste a calculé que l'adaptation nécessaire du protocole cryptographique prendrait un an environ. Les base pour la réduction des hypothèses de confiance seront approfondies dans une première étape.

Il est important pour la fiabilité du vote électronique de réduire les hypothèses de confiance. Cette réduction sera mise en œuvre à moyen terme.

L'approfondissement aura peu d'incidences financières pour la Confédération. L'adaptation du protocole cryptographique, par contre, entraînera des coûts considérables. Selon une première estimation de la Poste, les coûts suivants seront encourus :

- Coûts uniques pour l'adaptation du protocole cryptographique : 850 000 à 1 million de francs.

Il s'agira encore de régler la question du financement de ces travaux. La conception concrète et les coûts occasionnés par la mise en œuvre devront être examinés plus en détail au cours de l'étude. Sur la base des hypothèses actuelles concernant la conception et selon une première estimation, La Poste estime que la mise en œuvre entraînera les coûts suivants :

- Coûts uniques pour la poursuite de la mise en œuvre : de 700 000 à 900 000 francs
- Coûts récurrents pour le support, la maintenance et le fonctionnement (en moyenne) : 100 000 francs par an

Compte tenu de la répartition actuelle des compétences, ces coûts devraient être supportés par les cantons. Ceux-ci soulignent toutefois que les coûts liés à la première étape et à la mise en œuvre ultérieure excéderaient les ressources dont ils disposent. Il s'agira donc d'envisager un cofinancement par la Confédération.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
A.6	Approfondissement des informations servant de base à l'introduction d'un mécanisme de vérifiabilité supplémentaire dont l'efficacité ne repose pas sur les hypothèses de confiance actuelles	Etude : 1 an après la reprise des essais Proposition au CoPil VE : jusqu'à 2 ans après la reprise des essais	Etude : ChF avec la participation des cantons

Objectif et description de la mesure

Afin d'accroître la diversité, on étudiera plus avant les possibilités de prévoir un mécanisme de vérifiabilité supplémentaire. Il conviendra ainsi d'examiner si et de quelle manière il serait possible de mettre à la disposition des électeurs un instrument de vérifiabilité qui s'ajouterait à ceux qui ont été fournis par le fabricant. Un tel mécanisme pourrait par exemple être mis en place sous la forme d'un tableau d'affichage public (*Public Bulletin Board*), qui permettrait de rendre publiques les données relatives au vote tout en respectant sa confidentialité et permettrait aux votants, à l'aide d'un second dispositif (p. ex. un téléphone portable), de vérifier si leur vote est bien parvenu sur une ou plusieurs instances indépendantes du fournisseur. De cette manière, l'efficacité de la vérifiabilité individuelle ne dépendrait pas de la fiabilité de l'imprimerie ou des composants de contrôle. Dans le cadre des vérifications faites au sens de la vérifiabilité universelle, les cantons pourraient s'assurer que tous les votes enregistrés par les instances indépendantes ont été pris en compte dans le dépouillement.

Dans un premier temps, il s'agira de développer une étude afin d'approfondir l'utilité d'un mécanisme supplémentaire ainsi que la forme de sa mise en œuvre éventuelle. Cette étude devra aborder les questions relatives à la mise en œuvre technique et, avec la participation des votants, les questions de renforcement de la confiance et d'acceptabilité. L'étude sera établie sous la responsabilité de la ChF.

Une fois ce travail préliminaire terminé, la ChF et les cantons soumettront au CoPil VE une proposition détaillée sur l'opportunité de mettre en place un tableau d'affichage public, et selon quelles modalités. Le financement devra être assuré en vue de la mise en œuvre.

Dialogue avec les milieux scientifiques

La publication des votes chiffrés sur un « tableau d'affichage public » a été envisagée comme un moyen supplémentaire de vérification des votes. Cette mesure, complémentaire aux codes de vérification, est décrite dans la littérature scientifique. Les experts considèrent certes que la mise en place d'un tel tableau d'affichage constituerait un instrument approprié pour renforcer la confiance, mais ils font également valoir que cette confiance serait compromise si des erreurs sont commises dans la conception ou la mise en œuvre, ou si les besoins des électeurs, notamment en termes de communication, de présentation visuelle ou de convivialité, ne sont pas pris en compte. Aussi a-t-il été proposé de mener des projets de sciences participatives au titre de mesures d'accompagnement d'essais éventuels. Il s'agira d'examiner plus en détail aussi bien les questions relatives au traitement des informations envoyées par les votants pour signaler des résultats de contrôles négatifs que les aspects de sécurité, en vue de développer une solution concrète.

Impact de la mesure et appréciation globale du CoPil VE

Dans le cadre du dialogue avec les milieux scientifiques, certains experts ont approfondi le sujet dans une étude du point de vue cryptographique et indiqué des approches possibles. Un nouvel approfondissement de ces travaux est nécessaire avant qu'il soit possible de prendre une décision quant à la mise en œuvre éventuelle d'un tel mécanisme de vérifiabilité supplémentaire. Plusieurs aspects relatifs à la conception possible ainsi qu'aux avantages et aux inconvénients d'une telle solution sont encore ouverts à l'heure actuelle. L'étude devra notamment examiner de manière plus approfondie les questions de convivialité et de communication avec les électeurs. L'établissement de cette étude entraînera pour la Confédération des coûts d'importance moyenne, et aucune incidence financière pour les cantons.

La conception et les coûts associés à la mise en œuvre devront être examinés plus en détail dans le cadre de l'étude. Sur la base d'hypothèses faites pour la conception et selon une première estimation, la mise en œuvre devrait entraîner les coûts suivants :

- Coûts uniques : 600 000 francs
- Coûts récurrents (en moyenne) : 200 000 francs par an

La responsabilité de la mise en œuvre et donc du financement devra être éclaircie dans le cadre de l'étude. Les cantons font valoir que les coûts de mise en œuvre excéderaient les ressources dont ils disposent. Il s'agira donc d'envisager un cofinancement par la Confédération.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
A.7	Amélioration des capacités de détection (monitoring) et d'investigation (investigation numérique) des incidents	Définition des exigences et du processus d'amélioration : reprise des essais	Définition des exigences : ChF Processus d'amélioration : fournisseur, cantons

Objectif et description de la mesure

Les systèmes de vote électronique doivent permettre de détecter et d'investiguer efficacement les incidents, tels que les soupçons de manipulation des votes ou les attaques contre le système. L'ensemble du système devra être conçu et développé de telle sorte que la survenance d'incidents puisse être anticipée et que soient utilisés des outils appropriés à l'investigation de ces incidents (*forensic readiness*). Les informations collectées et stockées devront pouvoir être utilisées comme preuves numériques dans le cadre d'enquêtes sur des incidents et de procédures judiciaires. Le droit fédéral actuel contient certains principes applicables à la détection et au signalement des incidents et des failles de sécurité ainsi qu'à leur traitement et à leur résolution (ch. 3.2 de l'annexe de l'OVotE).

Les exigences actuelles en matière de collecte de traces seront précisées comme suit en vue de la reprise des essais : des logs cohérents seront établis à travers tous les éléments du système pour la détection et l'investigation des incidents ; ces logs devront être collectés, transférés et stockés d'une manière interdisant leur manipulation ; leur contenu devra être défini avec l'objectif de pouvoir conduire une investigation efficace des incidents. Le secret du vote doit être garanti.

Dans un deuxième temps et dès la reprise des essais sera défini et mis en œuvre un processus d'amélioration en continu pour la détection et l'investigation des incidents. Il y aura lieu de tenir compte notamment des aspects suivants :

- Il y aura un échange ouvert entre la Confédération, les cantons et les fournisseurs de systèmes.
- Des analyses portant sur l'adéquation des systèmes de monitoring et d'investigation seront effectuées régulièrement. Elles prendront en compte les scénarios définis dans la convention de crise. La participation d'experts en forensique à ces analyses, permettra d'apporter des améliorations plus efficaces.
- Les éléments résultant de l'analyse seront pris en compte dans le cadre de l'amélioration des instruments et des processus.

Dialogue avec les milieux scientifiques

Pour les experts, il est important que le système soit mis en place de manière à permettre la détection et l'investigation des incidents. Il s'agirait de s'assurer que les informations nécessaires soient générées de manière traçable tout au long du processus, sans violation du secret du vote. Des instruments appropriés devraient être utilisés pour collecter les informations et des simulations d'investigations devraient être effectuées régulièrement pour vérifier que les bonnes informations ont été collectées et qu'il soit possible d'y accéder de manière traçable.

Impact de la mesure et appréciation globale du CoPil VE

Cette mesure doit permettre la mise en place d'un échange ouvert entre la Confédération, les cantons et les fournisseurs de systèmes afin d'améliorer en continu le monitoring et la forensique. Les bases légales devront être précisées de manière à imposer des exigences claires concernant les éléments nécessaires à la détection et à l'investigation correctes des incidents. La *forensic readiness* du système sera ainsi améliorée et la confiance dans le canal de vote électronique renforcée.
La mise en œuvre de cette mesure n'aura aucune incidence financière pour la Confédération. Comme il s'agit d'une précision des exigences, les cantons ne s'attendent pas à des coûts supplémentaires. Toutefois, le processus d'amélioration qui doit être mis en œuvre dans le cadre de la mesure pourrait entraîner des coûts d'un montant encore indéterminé.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
A.8	Création d'un plan d'action commun de la Confédération et des cantons	Reprise des essais	ChF / cantons

Objectif et description de la mesure

La Confédération et les cantons se dotent d'un plan d'action commun. Le plan d'action reflète les décisions relatives à la restructuration de la phase d'essais et indique les mesures déjà mises en œuvre pour la reprise des essais et celles qui doivent être utilisées pour développer le vote électronique à moyen ou long terme. Lorsque cela est possible, il convient d'indiquer les délais de mise en œuvre des mesures ou les premières étapes prévues. Le CoPil VE adoptera le plan d'action sous la forme d'une déclaration d'intention et le publiera. La publication paraît au plus tard lors de la reprise des essais. Ce plan sera revu régulièrement, afin de garantir le maintien de la sécurité compte tenu des dernières évolutions en la matière.

Dialogue avec les milieux scientifiques

Les experts s'accordent à dire qu'il est nécessaire d'agir et que des mesures appropriées doivent être prises. Certaines de ces mesures seront coûteuses et leur mise en œuvre prendra du temps.

Impact de la mesure et appréciation globale du CoPil VE

Un plan d'action publié est un instrument utile pour montrer au public et à tous les acteurs impliqués les développements et travaux prévus. La tenue d'un plan d'action n'aura de conséquences financières directes ni pour la Confédération ni pour les cantons. Le coût des mesures à mettre en œuvre devra être indiqué pour chaque mesure.

B. Surveillance et contrôle efficaces

N°	Mesure	Calendrier mise en œuvre	Responsabilité
B.1	Modification des compétences dans le cadre de l'évaluation de la conformité du système et des processus qui l'entourent	Reprise des essais	ChF

Objectif et description de la mesure

L'expérience de 2019 a montré que les exigences actuelles en matière de contrôle des systèmes et des processus n'ont pas eu les effets souhaités. La publication du code source et un examen indépendant réalisé ultérieurement ont révélé des failles de sécurité graves que les audits et certifications précédents n'avaient pas permis de détecter. La présente mesure et la mesure B.2 modifient respectivement les compétences et la conception des contrôles des systèmes, afin de garantir l'efficacité et la crédibilité des contrôles.

L'indépendance entre l'organisme d'audit et l'entité auditée joue un rôle important dans le cadre de cette modification des compétences. C'est pourquoi la répartition des responsabilités entre la Confédération et les cantons sera revue de façon que la Confédération assume davantage de responsabilités et un rôle plus direct dans l'audit des systèmes. Les compétences seront modifiées comme suit :

Contrôles selon l'annexe à l'OVotE	Responsabilités actuelles	Responsabilités à l'avenir
5.1 Contrôle du protocole cryptographique	Responsabilité : Canton Mandant : Fournisseur Mandataire : Organe accrédité	Responsabilité : ChF Mandant : ChF Mandataire : Experts crypto
5.2 Contrôle des fonctionnalités	Responsabilité : Canton Mandant : Fournisseur Mandataire : Organe accrédité	Responsabilité : ChF Mandant : ChF Mandataire : Experts crypto et développement
5.3 Contrôle de l'infrastructure et de l'exploitation	Responsabilité : Canton Mandant : Fournisseur	*Infrastructure du fournisseur pour la certification ISO 27001* Responsabilité : Canton

	Mandataire :	Organe accrédité	Mandant : Mandataire :	Fournisseur Organe accrédité (ISO 27001)
			Infrastructure du fournisseur et du canton pour les aspects de l'OVotE Responsabilité : Mandant : Mandataire :	 ChF ChF Experts crypto et experts opérationnel
5.4 Contrôle des composants de contrôle	Responsabilité : Mandant : Mandataire :	Canton Fournisseur Organe accrédité	Responsabilité : Mandant : Mandataire :	ChF ChF Experts crypto et développement
5.5 Contrôle de la protection contre les tentatives d'intrusion dans l'infrastructure	Responsabilité : Mandant : Mandataire :	Canton Fournisseur Organe accrédité	Responsabilité : Mandant : Mandataire :	ChF ChF Experts sécurité
5.6 Contrôle concernant les imprimeries	Responsabilité : Mandant : Mandataire :	Canton Canton Organe accrédité	Responsabilité : Mandant : Mandataire :	ChF ChF Experts crypto et experts opérationnel

Le fournisseur du système continuera ainsi d'être responsable des contrôles liés à l'exploitation du système dans ses centres informatiques (certification ISO 27001 prévue au ch. 5.3 de l'annexe de l'OVotE). Il n'y aura plus à l'avenir de certification plus poussée par les services accrédités par le Service d'accréditation suisse (SAS). La Confédération aura la compétence de vérifier que les exigences relatives au système et aux processus sous-jacents sont remplies. Des experts indépendants seront chargés de procéder aux vérifications.

La ChF adaptera l'OVotE et son annexe en vue de la reprise.

Dialogue avec les milieux scientifiques

Les experts ont souligné que les contrôles indépendants devraient être commandés par un comité indépendant ou par la Confédération. Une certification n'aurait de sens que dans le cadre d'un audit de l'exploitation (certification selon la norme ISO 27001). Les autorités devraient s'appuyer sur des audits indépendants réalisés par des personnes possédant les compétences nécessaires. Des compétences appropriées en matière d'audit sont bien plus précieuses qu'une certification des systèmes de vote électronique. Les cryptographes devraient également participer à la vérification du code source et de l'exploitation. L'audit devrait suivre une approche globale de façon à prévenir toute lacune. Les experts soulignent en outre tout particulièrement l'importance du contrôle public (*public scrutiny*).

Impact de la mesure et appréciation globale du CoPil VE

Il est possible de garantir l'efficacité des contrôles en faisant en sorte que la Confédération confie à l'avenir la plupart des audits à l'extérieur. Cette mesure est considérée comme importante et utile, avec la préparation du concept d'audit (mesure B.2).

Le financement des audits incombera à l'organisme compétent dans le cas particulier. Aussi la modification des compétences aura-t-elle un impact financier élevé pour Confédération. Les cantons resteront responsables du contrôle de l'infrastructure du fournisseur de système (certification selon ISO 27001). Cela permettra d'éliminer les coûts précédemment dus à une certification par un organisme accrédité par le SAS. Les cantons estiment cependant qu'il n'en résultera pas pour eux d'économies directes (le transfert des compétences suppose une préparation plus complète de la part du fournisseur du système, tandis que les frais de personnel pour la réalisation du contrôle restent inchangés).

La modification des compétences influe sur les processus qui unissent la Confédération, les cantons et les fournisseurs de systèmes, ainsi que sur la procédure d'autorisation (voir mesure B.9). La ChF transmettra au fur et à mesure aux cantons les rapports d'audit et partagera avec eux les premières évaluations qu'elle porte sur les résultats des contrôles, ce qui fournira aux cantons les informations nécessaires à l'évaluation de la demande qu'ils adresseront à la Confédération. La ChF veillera ainsi à ce que les cantons soient associés aux audits et elle échangera régulièrement des informations avec eux.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
B.2	Elaboration d'un concept d'audit pour l'évaluation de la conformité du système et des processus qui l'entourent	Reprise des essais	ChF en collaboration avec les cantons et le fournisseur du système

Objectif et description de la mesure

La mesure B.1 revoit les responsabilités en matière d'audit des systèmes et des processus. L'établissement d'un concept d'audit permettra de visualiser ces nouvelles compétences, garantira des audits exhaustifs et se traduira de manière générale par une plus grande efficacité des contrôles. Le concept d'audit sera conçu de manière à garantir un passage en revue complet des exigences de sécurité.

Le concept d'audit devra notamment inclure les aspects suivants :

- Définition claire de la portée des différents domaines d'examen : seront ainsi déterminés leur périmètre et la durée de validité des contrôles.
- Perméabilité entre les différentes domaines d'examen : cette perméabilité garantira des contrôles cohérents et complets.
- Mandat d'experts qualifiés et indépendants.
- Publication des rapports d'audit (voir mesure C.4).

Les audits du système doivent être effectués à un stade précoce afin de laisser suffisamment de temps avant la mise en service du système pour qu'il soit possible de remédier aux non-conformités et d'effectuer un nouveau contrôle (voir la mesure B.3 pour le traitement des non-conformités).

Le concept d'audit sera développé par la ChF. Les contrôles préalables à la reprise des essais seront effectués sur la base de ce dernier. La ChF pourra consulter des experts externes pour le développement du concept.

Dialogue avec les milieux scientifiques

Voir le commentaire figurant sous la mesure B.1.

Impact de la mesure et appréciation globale du CoPil VE

Voir le commentaire figurant sous la mesure B.1. Pour ce qui est du développement d'un concept d'audit, son impact financier pour la Confédération sera peu élevé. Le recours à des experts externes pourra éventuellement occasionner des coûts. La mesure n'aura pas d'incidences financières pour les cantons.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
B.3	Elaboration et mise en œuvre d'un processus de traitement des non-conformités	Reprise des essais	ChF en collaboration avec les cantons et le fournisseur du système

Objectif et description de la mesure

Les non-conformités, telles que des failles du système ou des processus qui l'entourent, peuvent être détectées à tout moment. Si des non-conformités sont découvertes ou suspectées peu avant ou pendant l'utilisation du vote électronique, il est très important de disposer d'une procédure claire pour leur traitement. Les non-conformités ne doivent pas toutes empêcher l'utilisation du système, et il s'agit de les évaluer en fonction de leur impact sur les risques et de vérifier s'il est possible de réduire au moyen d'autres mesures le risque associé à la non-conformité. La mise en place d'un processus de traitement des non-conformités vise à prévenir autant que possible les incertitudes face à une non-conformité et à garantir que l'utilisation du vote électronique se fera conformément aux exigences de l'OVotE.

Avant que les essais ne reprennent, la ChF élaborera avec les cantons et le fournisseur de système un processus de traitement des non-conformités avérées ou présumées, tenant compte des aspects suivants :

- Définition de ce qu'est une non-conformité : il est précisé quel type de non-conformité déclenche le processus.
- Définition de critères : sont précisés les critères appliqués pour le traitement des non-conformités. Les non-conformités sont évaluées en fonction de leur impact sur les risques, les risques résultant d'un retrait du système étant eux aussi pris en compte. Il est en principe plus facile d'utiliser un

système de vote électronique lorsque les non-conformités concernent non pas le système lui-même, mais les processus qui l'entourent. Si une non-conformité devait être considérée comme conciliable avec une mise en service, il y a lieu de prévoir sa correction et, si nécessaire, de la reprendre dans le plan d'action de la Confédération et des cantons (voir mesure A.8).

- Détermination des acteurs et de leurs rôles respectifs : il y a lieu de préciser les rôles que joueront la Confédération, les cantons, le fournisseur de système et le cas échéant d'autres acteurs, ainsi que les modalités de leur collaboration. Des experts indépendants seront associés au traitement des non-conformités.

Dialogue avec les milieux scientifiques

Les experts ont souligné l'importance d'un processus clair pour le traitement des non-conformités. Ils sont d'accord pour considérer qu'une non-conformité ne doit pas systématiquement empêcher d'utiliser le vote électronique, et que des risques minimes peuvent être admis. Cela suppose toutefois que les risques soient appréciés correctement, ce qui est parfois difficile. Il serait également possible de prendre la gravité de la non-conformité comme critère de décision. Des comparaisons avec des risques déjà admis peuvent à cet égard se révéler utiles. Il faut également tenir compte de ce que l'abandon du vote électronique entraîne dans les faits pour une partie des électeurs suisses de l'étranger la perte du droit de vote, et qu'il se traduira par un recours accru au vote par correspondance, lui aussi non exempt de risques. Plus une non-conformité affecte le système et moins elle est limitée aux processus qui entourent ce dernier, et plus vite il faudra la corriger. Les erreurs qui touchent le protocole cryptographique ou sa mise en œuvre dans le code source ne doivent en aucun cas être acceptées.

Impact de la mesure et appréciation globale du CoPil VE

La définition d'une procédure de traitement des non-conformités est une mesure importante. Un processus décisionnel clair et intégrant les critères à prendre en compte pour traiter les non-conformités bénéficiera à tous les acteurs impliqués. La mise en œuvre de cette mesure n'aura aucune incidence financière pour les cantons. Quant à la Confédération, elle aura à supporter tout au plus des coûts minimes liés au recours à des experts externes.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
B.4	Renouvellement et amélioration du guide pour l'appréciation des risques	Reprise des essais	ChF en collaboration avec les cantons et le fournisseur du système

Objectif et description de la mesure

Il s'agit de revoir et d'améliorer les principes et les prescriptions qui encadrent aujourd'hui l'appréciation des risques. Les appréciations des risques menées par la ChF, par les cantons et par le fournisseur du système (voir mesure B.5) s'appuieront sur un guide. Celui-ci décrira l'approche générale à adopter à cet égard et précisera les compétences respectives. Le choix de la méthode d'appréciation des risques restera à la discrétion des acteurs concernés. Le guide précisera notamment les aspects suivants :

- Catalogue d'actifs informationnels
- Catalogue de menaces (basé sur la liste des menaces du point 3.1 de l'annexe de l'OVotE)
- Catalogue de mesures de mitigation
- Responsabilités en matière de protection des actifs informationnels

Le guide devra par ailleurs tenir compte de la longueur des clés de chiffrement, du vote multiple par différents canaux, de l'achat de votes, de la *long term privacy* et de la dépendance à l'égard d'un fournisseur unique.

Le guide sera établi par la ChF en collaboration avec les cantons, les fournisseurs de systèmes et des experts en sécurité informatique. Il sera publié avant la reprise des essais afin de renforcer la transparence et la confiance. En outre, il donnera ainsi la possibilité au public de donner son avis. Le guide devra être revu périodiquement et adapté au besoin.

Dialogue avec les milieux scientifiques

L'établissement d'un guide destiné à encadrer les appréciations des risques a été évoquée dans le cadre du dialogue avec les experts. Ceux-ci estiment qu'un tel guide doit être élaboré par la Confédération (en collaboration avec les cantons, les fournisseurs de systèmes et, si nécessaire, des experts

externes) afin d'asseoir sur un socle cohérent l'appréciation des risques et leur couverture complète. Le choix de la méthode d'appréciation devrait continuer à être laissé aux organismes concernés. Le guide devrait dresser la liste des menaces, proposer des mesures de réduction des risques et définir les responsabilités. Il serait publié pour permettre un retour d'information de la part des experts externes.

Impact de la mesure et appréciation globale du CoPil VE

L'établissement du guide permettra de disposer d'un socle efficace et uniforme pour la conception des appréciations des risques, pouvant servir de référence à tous les acteurs concernés. Cela simplifiera les processus. Cette mesure aura un impact financier minime pour la Confédération, et sera sans incidences financières directes pour les cantons. Le guide devra être disponible avant la mise en œuvre de la mesure B.5.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
B.5	Elaboration et mise en œuvre d'un nouveau processus d'appréciation des risques pour des systèmes complètement vérifiables	Reprise des essais	ChF, cantons, fournisseur du système

Objectif et description de la mesure

Les appréciations des risques prévues à ce jour seront restructurées. À l'avenir, ce ne sont plus seulement les cantons, mais tous les acteurs concernés (ChF, cantons, fournisseurs de systèmes) qui devront préparer leur propre appréciation des risques pour leur domaine de responsabilité. Les compétences et la marche à suivre seront régies par le guide prévu dans la mesure B.4. Les appréciations des risques devront refléter la situation actuelle et intégrer en continu les développements et connaissances les plus récents. Les appréciations des risques seront revues au moins une fois par an et à chaque modification importante du système. Il s'agira en outre de vérifier avant chaque scrutin si se présentent des risques spécifiques ou s'il y a une aggravation des risques existants. Si les mesures de réduction des risques ne peuvent être mises en œuvre immédiatement, elles devront être intégrées dans le plan d'action (mesure A.8). Des experts indépendants seront associés à l'appréciation des risques.

La ChF adaptera en conséquence l'OVotE. Les appréciations des risques de l'ensemble des acteurs concernés devront être disponibles avant toute reprise des essais.

Dialogue avec les milieux scientifiques

Les experts sont favorables à ce que chaque acteur (ChF, cantons, fournisseurs de systèmes) établisse une appréciation des risques pour son domaine de responsabilité. Ils conviennent que les risques doivent être régulièrement évalués à l'aide d'une méthode systématique et exhaustive. L'appréciation des risques devrait être revue au moins une fois par an et suite à tout changement significatif apporté au système. Une revue spécifique en vue d'un scrutin (tous les trois mois) est souhaitable. Toutefois, un intervalle de trois mois est quelque peu exigeant et il pourrait être utile de revenir à un intervalle plus long après quelques années. Le choix de la méthodologie utilisée est d'une importance secondaire. La moitié des experts ont jugé particulièrement difficiles à gérer les risques découlant de la dépendance à l'égard de fournisseurs ou fabricants tiers (risques de la chaîne d'approvisionnement, ou *supply chain risks*). Une majorité d'entre eux estiment qu'il pourrait être utile de nommer un comité d'experts qui serait chargé d'accompagner le processus de gestion des risques. Les experts se sont entretenus par ailleurs des différents avantages et inconvénients liés à la publication des appréciations des risques. Ils recommandent à cet égard de ne pas publier immédiatement l'appréciation détaillée des risques. Il pourrait être utile de publier des graphiques et des données statistiques ainsi que des informations sur la gouvernance et de rendre transparentes les règles pour une possible publication ultérieure de l'appréciation détaillée des risques.

Impact de la mesure et appréciation globale du CoPil VE

Il est possible de garantir une gestion efficace des risques en veillant à ce que chaque acteur évalue et traite les risques qui relèvent de son domaine de responsabilité. Le guide prévu dans la mesure B.4 définit la répartition des responsabilités et une base commune pour l'appréciation des risques. Il est important qu'il y ait en permanence un échange et une concertation entre les différents acteurs, de façon à mutualiser les expériences (par exemple les expériences du Canton de Fribourg avec la méthode OCTAVE Allegro d'évaluation des risques). La Confédération et les cantons peuvent bénéficier de l'assistance d'experts externes pour identifier et évaluer les risques.

La mise en œuvre de cette mesure peut entraîner ponctuellement des efforts supplémentaires pour la Confédération et les cantons, mais il est possible de les couvrir avec les ressources existantes. Le recours à des spécialistes externes peut éventuellement entraîner des coûts, mais peu élevés.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
B.6	Renouvellement de la gestion de crise avec conduite d'exercices de crise	Reprise des essais	ChF (lead), cantons et fournisseur du système

Objectif et description de la mesure

Une gestion de crise efficace et fonctionnelle est un aspect important de la mise en œuvre d'un système de vote électronique fiable et sûr. Jusqu'à présent, la Confédération et les cantons ont défini dans une convention de crise la manière dont l'information, la collaboration et la communication doivent se dérouler en cas d'incident lié au vote électronique. Cette pratique sera renouvelée afin de tenir compte des développements intervenus en matière de vote électronique et d'améliorer l'efficacité de la gestion des crises. Il s'agit en conséquence d'établir une nouvelle convention de crise, sous la forme d'un contrat-cadre présentant les propriétés suivantes :

- Convention tripartite : la convention de crise sera conclue entre la ChF, les cantons utilisateurs et le fournisseur du système.
- Processus, rôles et tâches : seront définis les processus de gestion des crises ainsi que les rôles et les tâches des acteurs impliqués.
- Communication : la convention de crise prévoira un processus de communication entre les acteurs impliqués (communication interne) et un processus de coordination de la communication vis-à-vis de l'extérieur (communication externe). Une plate-forme de communication appropriée sera mise en place pour la communication entre les acteurs concernés.
- Exercices : la gestion de crise fera l'objet d'exercices à intervalles à définir afin d'améliorer les processus et la coopération dans la gestion des crises.
- La convention de crise adaptera les scénarios de crise aux appréciations des risques nouvellement applicables aux systèmes entièrement vérifiables. Les structures existantes mises en place par la Confédération, les cantons et les fournisseurs de systèmes seront maintenues autant que possible dans la gestion de crise.

Les nouvelles conventions de crise devront avoir été élaborées et signées avant la reprise des essais. Les premiers exercices pratiques pourront avoir lieu après cette reprise.

Dialogue avec les milieux scientifiques

Les experts ont souligné que des processus clairement définis ainsi que des plans d'action et de communication sont essentiels pour une bonne gestion des crises. Ils ont également proposé que soient associés à la gestion de crise non seulement le service fédéral compétent, les cantons concernés et le fournisseur du système, mais aussi d'autres services fédéraux (GovCERT / MELANI), des spécialistes en communication et des experts techniques indépendants.

Impact de la mesure et appréciation globale du CoPil VE

Cette mesure est nécessaire pour adapter la gestion de crise à la situation actuelle et pour permettre un processus d'amélioration continue. La mise en œuvre de cette mesure aura un impact financier réduit pour la Confédération. Quant aux cantons, ils n'auront à supporter aucun coût externe supplémentaire pour la mise en œuvre et l'implémentation de la gestion de crise et pour les exercices.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
B.7	Intégration du vote électronique dans les infrastructures critiques de la Confédération	Reprise des essais	ChF (lead), cantons et fournisseur du système

Objectif et description de la mesure

Les infrastructures critiques au sens de la Stratégie nationale de protection des infrastructures critiques bénéficient d'un soutien accru de la part du Centre d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) et de l'Équipe nationale d'intervention en cas d'urgence informatique

(GovCERT). Ce soutien serait précieux pour l'analyse des menaces et l'investigation des incidents liés au vote électronique. Cette mesure vise à définir la coopération entre la ChF, les cantons, le fournisseur de système et GovCERT / MELANI en matière de vote électronique afin de garantir un accès prioritaire pour le traitement des incidents. Cette collaboration devrait également être prise en compte dans la gestion des crises.

Dialogue avec les milieux scientifiques

La question du vote électronique vu comme faisant partie des infrastructures critiques n'a pas été expressément abordée dans le cadre du dialogue avec les milieux scientifiques. Les experts ont cependant indiqué qu'une coopération avec GovCERT / MELANI constituerait un avantage.

Impact de la mesure et appréciation globale du CoPil VE

Cette mesure n'aura d'incidences financières ni pour la Confédération ni pour les cantons.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
B.8	Poursuite du développement du contrôle de la plausibilité des résultats du vote électronique	Reprise des essais : premier échange Examen d'une méthode standardisée : 2022	Cantons

Objectif et description de la mesure

Le droit actuel prévoit que les résultats des scrutins organisés par voie électronique sont contrôlés quant à leur plausibilité (art. 27*i*, al. 1, ODP). Ce contrôle de plausibilité est destiné à fournir des indices donnant à penser que des erreurs ont été commises involontairement dans la détermination des résultats ou que ceux-ci ont été manipulés. Il est prévu d'utiliser à cet effet des méthodes statistiques, dans la mesure où la base de données le permet (ch. 3.2.8 de l'annexe de l'OVotE). Les cantons contrôlent la plausibilité des résultats du vote électronique de manières diverses. Il s'agit donc d'intensifier les échanges entre les cantons et avec la ChF, de façon que les différentes expériences et approches puissent être discutées dans une perspective de bonnes pratiques. Il sera examiné en outre s'il est possible de développer une méthode statistique standardisée, et sous quelle forme. La mise en place d'une procédure standardisée constituerait un outil supplémentaire permettant d'obtenir des indices de dysfonctionnements ou manipulations possibles. La méthode devra être applicable à la situation spécifique de chaque canton. Il est prévu de publier les résultats du vote électronique pour les scrutins fédéraux de façon à assurer la transparence du contrôle de plausibilité (voir mesure C.5). Il conviendra également de vérifier quelles informations pourront être publiées en ce qui concerne les contrôles de plausibilité des cantons. Ces mesures permettront au public d'évaluer les contrôles de la plausibilité des résultats du vote électronique effectués par les autorités.

Un premier échange entre les cantons et avec la ChF sur les pratiques antérieures devrait avoir lieu en vue de la reprise de la phase d'essai. Les vérifications relatives à la mise en place d'une méthode standardisée et l'examen des informations qui devraient être publiées à l'avenir en ce qui concerne les contrôles de plausibilité effectués par les cantons devraient être effectués d'ici à 2022.

Dialogue avec les milieux scientifiques

La question de l'emploi d'une méthode statistique standardisée pour les contrôles de plausibilité a été discutée dans le cadre du dialogue avec les milieux scientifiques. Une telle méthode n'existe pas encore, mais les experts pensent néanmoins qu'il serait possible de la développer. Ils estiment du reste que si une méthode statistique ne permet pas de détecter une manipulation, les contrôles de plausibilité peuvent néanmoins fournir des indices d'irrégularités, sur la base desquels peuvent être menées des investigations sur la présence de possibles manipulations. L'absence d'indices ne garantit toutefois pas l'absence de manipulations.

Impact de la mesure et appréciation globale du CoPil VE

Il faut agir pour développer davantage les contrôles de plausibilité déjà prescrits dans les cantons. La mise en œuvre de cette mesure tiendra compte des conséquences pour les autres canaux de vote et des efforts déjà entrepris dans plusieurs cantons pour améliorer de manière générale le contrôle de la plausibilité des résultats des votations et des élections.

Cette mesure n'a pas d'incidence financière pour la Confédération. Pour ce qui est des cantons, les incidences financières dépendent de la possibilité de développer une telle méthode et de la nature de cette dernière, mais elles devraient être plutôt faibles.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
B.9	Adaptations de la procédure d'autorisation	Reprise des essais	ChF avec la participation des cantons

Objectif et description de la mesure

La mise en œuvre de plusieurs mesures en vue de la reprise des essais rend nécessaire d'adapter les processus inhérents à la procédure d'autorisation. Il s'agit en particulier des mesures visant à revoir les compétences en matière d'audits indépendants (mesure B.1) et de la précision des exigences relatives à la transparence (mesures C.2 et C.3). Il conviendra en outre de tenir compte aussi bien du recours à des experts indépendants dans le cadre de la procédure d'autorisation que de la gestion en continu des risques. Le schéma actuel de la procédure d'autorisation prévue par l'ODP (autorisation générale accordée par le Conseil fédéral, agrément accordé par la ChF) sera conservé en vue de la reprise des essais.

Pour mettre en œuvre cette mesure, la ChF adaptera les processus inhérents à la procédure d'autorisation. Elle révisera à cette fin les exigences prévues par cette procédure. La ChF examinera également dans quelle mesure la décision d'autorisation générale du Conseil fédéral peut être divisée en une partie liée au système et une partie spécifique au canton.

Dialogue avec les milieux scientifiques

La question de la forme que doit prendre la procédure d'autorisation n'a pas été expressément abordée dans le cadre du dialogue avec les milieux scientifiques. Mais les experts accordent de manière générale une grande importance à ce que soient associés à l'évaluation des systèmes de vote électronique des personnes et des organismes compétents et indépendants.

Impact de la mesure et appréciation globale du CoPil VE

Il est nécessaire d'adapter la procédure d'autorisation, notamment pour tenir compte du nouvel audit indépendant. Il est indispensable que la ChF et les cantons concernés se concertent à un stade précoce afin de coordonner les processus.

Comme expliqué dans la mesure B.1, la ChF veillera à ce que les cantons soient associés aux audits et elle échangera régulièrement des informations avec eux. En divisant la décision d'autorisation générale en une partie spécifique au système et une partie spécifique au canton, une certaine sécurité de planification sera apportée aux cantons qui demandent une autorisation générale pour un système déjà approuvé. S'ils utilisent la même version du système que les autres cantons, ils peuvent être sûrs que la partie générique du système répond aux exigences fédérales.

La mise en œuvre de cette mesure n'aura d'incidences financières ni pour la Confédération ni pour les cantons.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
B.10	Examen à long terme des processus, rôles et des tâches	Long terme	GT Avenir VE

Objectif et description de la mesure

Les responsabilités, les rôles et les tâches de la Confédération, des cantons et des fournisseurs de systèmes influent directement sur la conception des systèmes de vote électronique considérée sous l'angle de la sécurité. Il est prévu que ceux-ci feront l'objet d'un réexamen à long terme pour être intégrés dans une stratégie. Il sera possible dans ce contexte d'envisager des ajustements de fond de ces responsabilités, rôles et tâches. La Confédération et les cantons peuvent élaborer des mesures qui tiennent compte de la situation nouvelle en ce qui concerne le nombre de fournisseurs de systèmes, la gouvernance et les besoins de financement du vote électronique. La répartition actuelle des tâches, des compétences et des responsabilités tient compte du partage fédéraliste des tâches en matière de droits politiques. Les processus, les rôles et les tâches doivent être développés et conçus de manière à ce que la sécurité puisse être assurée et renforcée de manière continue et ciblée. Il faut tenir compte des

compétences techniques et des ressources humaines disponibles aux niveaux fédéral et cantonal, ainsi que de la dépendance à l'égard du fournisseur du système.

La définition des questions à traiter et la mise en œuvre de la mesure devraient relever de la responsabilité du groupe de travail Avenir VE, qui sera chargé d'étudier les questions de long terme sur proposition de la Conférence des Chanceliers d'État. Ce groupe de travail devra examiner si, sur le plan des droits politiques, et pour quelles tâches, une centralisation accrue des structures en matière de vote électronique serait de nature à apporter une plus-value ultérieurement. Ces travaux seront intégrés dans la Stratégie globale de cyberadministration et dans les structures actuelles, et couvriront non seulement le vote électronique mais tous les aspects de la cyberdémocratie. Les cantons ont préparé un projet de mandat à confier au groupe de travail Avenir VE, et la Conférence des Chanceliers d'État décidera de la marche à suivre.

Dialogue avec les milieux scientifiques

Le réexamen des processus, des rôles et des tâches a été abordé dans le cadre du dialogue avec les experts scientifiques non pas comme une question à part entière, mais dans le contexte de mesures spécifiques (come les audits indépendants).

Impact de la mesure et appréciation globale du CoPil VE

La mise en œuvre de cette mesure n'aura d'incidences financières ni pour la Confédération ni pour les cantons.

C. Renforcement de la transparence et de la confiance

N°	Mesure	Calendrier mise en œuvre	Responsabilité
C.1	Limitation de l'électorat admissible pour les systèmes complètement vérifiables	Reprise des essais	ChF

Objectif et description de la mesure

Le Conseil fédéral a décidé, le 26 juin 2019, de renoncer momentanément à passer à la mise en exploitation du vote électronique et de prolonger la phase d'essai. À cet égard, les seuls systèmes qui seront utilisés à l'avenir seront des systèmes complètement vérifiables. Afin de souligner le caractère expérimental de cette phase, on maintiendra, au moyen de cette mesure, la limitation de l'électorat en vigueur jusqu'à présent, même si on utilise des systèmes complètement vérifiables.

La ChF adaptera les bases légales pour que, durant la phase d'essai, l'électorat autorisé à voter par voie électronique soit limité lors de l'utilisation de systèmes complètement vérifiables. Les plafonds seront de 30 % pour l'électorat cantonal et de 10 % pour l'électorat national. Le respect des plafonds cantonaux incombera aux cantons, comme c'était le cas jusqu'à présent (procédure d'enregistrement, recours au vote électronique dans des communes pilotes ou uniquement pour les électeurs suisses de l'étranger). Les électeurs suisses de l'étranger continueront de ne pas être comptabilisés dans le calcul des plafonds. Cette limitation s'appliquera à la prochaine étape de la phase d'essai afin que l'on puisse collecter des connaissances avec les systèmes complètement vérifiables et renforcer la confiance en instaurant le vote électronique par étapes.

Dialogue avec les milieux scientifiques

Plusieurs avis concernant la limitation de l'électorat ont été exprimés lors du dialogue avec les milieux scientifiques. La majorité des experts soutiennent la limitation durant la phase d'essai, estimant qu'il s'agit là d'une mesure destinée à réduire les risques. Par contre, les avis divergent sur la question de savoir si, par ailleurs, la limitation de l'électorat est de nature à renforcer la confiance. Deux groupes de tailles plus ou moins égales s'opposent : le premier estime que l'utilisation du vote électronique par un pourcentage relativement limité de l'électorat est propre à favoriser à long terme l'adhésion et la confiance de la population à l'égard du vote électronique ; le second est d'avis que la limitation de l'électorat n'a aucune influence sur la confiance ou qu'elle est même susceptible de faire reculer cette dernière si elle donne l'impression que le système est considéré comme n'étant pas fiable. Quoi qu'il en soit, la limitation ne doit être qu'une mesure provisoire.

Impact de la mesure et appréciation globale du CoPil VE

Cette mesure est un instrument efficace, parce qu'elle souligne qu'il s'agit d'une phase d'essai et que l'instauration du vote électronique se fera par étapes. C'est en poursuivant sur la lancée actuelle, à savoir en limitant l'électorat, que l'on renforcera la confiance dans le vote électronique. Les plafonds, à savoir 30 % de l'électorat cantonal et 10 % de l'électorat national, devront s'appliquer durant la première phase de la reprise des essais. Le relèvement ou le cas échéant l'abrogation des plafonds sera examiné quand les systèmes complètement vérifiables auront fait leurs preuves au cours d'une phase d'essai stable.

La mise en œuvre de cette mesure n'aura pas d'incidences financières pour la Confédération. Cette dernière garantira dans le cadre de la procédure d'autorisation, de concert avec les cantons requérants, le respect du plafond s'appliquant à l'électorat national. Les cantons devront mettre en œuvre des mesures destinées à garantir le respect des plafonds cantonaux, ce qui pourra entraîner des coûts moyens, suivant le choix de l'instrument (par ex. mise sur pied d'une procédure d'enregistrement). Les cantons qui ont prévu d'instaurer le vote électronique sur l'ensemble de leur territoire et qui n'ont pas encore mis en œuvre de mesures destinées à limiter l'électorat devraient s'attendre à des surcoûts.

La limitation de l'électorat pourrait dissuader certains cantons d'instaurer le vote électronique. Cela pourrait être le cas si, par exemple, le plafond national était déjà atteint ou si un canton ne souhaitait proposer le vote électronique qu'à la condition que l'ensemble de son électorat soit autorisé à voter par voie électronique. En pratique, il ne faut pas s'attendre, dans les années à venir, à ce que les plafonds proposés aient des conséquences restrictives de ce type. Dès que des restrictions seront perceptibles, il faudra réexaminer cette mesure.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
C.2	Précision des exigences concernant la publication du code source	Reprise des essais	Exigences : ChF Publication : Cantons, fournisseur

Objectif et description de la mesure

Les connaissances acquises suite à la publication du code source du système de la Poste ont montré qu'il faut prendre des mesures dans ce domaine. Il s'agit de préciser les exigences auxquelles doivent répondre les documents dont la publication est requiseafin de tenir compte notamment des aspects suivants :

- Le code source du logiciel, la documentation relative à ce dernier et les fichiers contenant les paramètres d'entrée pertinents doivent être publiés.
- Les guides et autres documentations complémentaires doivent être publiés afin que des personnes spécialisées puissent efficacement compiler, faire fonctionner et analyser le système dans leur propre infrastructure.
- La documentation concernant l'infrastructure, les logiciels tiers et les processus d'exploitation doit être publiée dans toute la mesure du possible. Les éléments essentiels doivent à tout le moins faire l'objet d'une synthèse.
- La présentation des documents publiés doit être conforme à la pratique courante.

Les exigences relatives aux conditions d'utilisation sont les suivantes :

- L'accès au code source est gratuit et anonyme. On ne demandera pas aux personnes souhaitant consulter les informations publiées de révéler leur identité.
- Le code source peut être utilisé à des fins idéales et notamment scientifiques, par exemple s'il s'agit d'échanger des informations pour rechercher des erreurs, ou encore de faire usage du droit de publication. Ce droit est accordé explicitement par le propriétaire.
- Quiconque respecte les conditions d'utilisation ne sera pas poursuivi en justice. Une violation des conditions d'utilisation ne sera poursuivie que si le code source ou des parties de celui-ci sont utilisés à des fins commerciales ou productives. Les conditions d'utilisation font référence à cette limitation de responsabilité.
- Il suffit de faire référence, dans les termes de la licence, aux conditions d'utilisation. Il convient si possible de renoncer aux déclarations d'intention de l'utilisateur.

La ChF remaniera ses exigences avant la reprise des essais. Le CoPil VE est favorable à la publication des futurs systèmes et composants de systèmes sous une licence *open source*. En outre, la Poste, en tant que fournisseur actuel du système, examine si le code source des composants de son système complètement vérifiable déjà développés peuvent également être placés sous une licence *open source*.

Dialogue avec les milieux scientifiques

Les experts insistent sur le fait que la transparence revêt une grande importance, car elle constitue le fondement de tout contrôle public efficace. La publication du code source et de la documentation le concernant, assortie d'aussi peu d'obstacles d'accès que possible, constitue à cet égard une mesure importante. Plusieurs possibilités d'améliorer les dispositions qui régissent actuellement la publication du code source ont fait l'objet de discussions. Il convient de renoncer absolument aux déclarations de confidentialité.

Les experts estiment que la publication du code source sous une licence *open source* est plus prometteuse que sa publication sous une licence propriétaire. Une licence *open source* permet d'atteindre plus efficacement les objectifs que sont la transparence, le contrôle public, la confiance de la population et la constitution d'une communauté de spécialistes. La publication sous une licence propriétaire permet certes d'atteindre également ces objectifs, mais pas dans la même mesure. C'est pourquoi les experts recommandent la publication sous une licence *open source* notamment parce qu'elle permet avant tout d'utiliser et de développer les éléments cryptographiques dans d'autres applications. Ainsi, une telle réutilisation pourrait profiter au développement et à la sécurité du vote électronique.

De nombreux experts plaident en faveur de la publication précoce du code source et de la documentation en la matière. À cet égard, on pourrait aussi publier une version préliminaire avant de publier la version finale, laquelle servirait durant la phase productive. Certains experts ont en outre indiqué que la documentation publiée devrait être de grande qualité et que toute modification devrait être visible. Les experts estiment par ailleurs qu'il faut publier non seulement le code source, mais aussi tous les documents nécessaires pour comprendre le fonctionnement et l'utilisation du système. Enfin, il doit être possible de tester le système sur ses propres ordinateurs.

Impact de la mesure et appréciation globale du CoPil VE

La publication du code source est importante dans l'optique du contrôle public et la constitution d'une communauté en la matière composée de spécialistes doit être promue. La publication du code source requiert la prise de mesures. Avant de reprendre les essais, il faut préciser et adapter les exigences applicables aux documents qui doivent être publiés et aux conditions d'utilisation, comme cela est décrit dans la mesure.

Indépendamment de la publication du code source et des modalités de cette dernière, il convient de déterminer si le code source d'un système de vote électronique doit être publié sous une licence *open source*. En termes simples, une telle licence permet à des tiers d'utiliser, de modifier et d'exploiter le code source à leurs propres fins (y compris productive). Le CoPil VE est favorable à la publication des futurs systèmes et composants sous une licence *open source* Toutefois, la publication du code source du système de la Poste sous une licence *open source* n'est pas une condition préalable à l'utilisation de ce dernier. Cependant, avec la Poste en tant que fournisseur actuel du système, on examinera si le code source des composants de son système complètement vérifiable déjà développés peuvent également être placés sous une licence *open source*.

La publication du code source va coûter très cher, mais la mise en œuvre de cette mesure ne devrait pas avoir, dans l'immédiat, des incidences financières directes supplémentaires pour la Confédération et les cantons.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
C.3	Gestion d'un programme de bug bounty	Reprise des essais	Exigences : ChF Mise en œuvre : Cantons, fournisseur

Objectif et description de la mesure

Dans le souci d'associer des spécialistes indépendants au contrôle public, on mettra en place un programme de bug bounty portant sur le code source et la documentation publiés relatifs aux systèmes de vote électronique. Ce programme répondra, entre autres, aux exigences suivantes :

- Le fournisseur du système de vote électronique gère un programme de bug bounty qui fonctionne en principe sans interruption. Le programme doit commencer avant la soumission au Conseil fédéral d'une demande définitive en vue d'obtenir une autorisation générale (environ trois mois).
- Le signalement d'un défaut donne droit au versement d'une indemnité financière en rapport avec la gravité du défaut constaté. Le barème des indemnités doit se baser sur le barème utilisé lors du test public d'intrusion réalisé en 2019.
- Les participants peuvent analyser le code source dans leur propre infrastructure à l'aide du système en fonction. Pour obtenir une indemnité, il suffit de mettre au jour des défauts à l'aide du code source ; il n'est pas nécessaire qu'une attaque réussie ait eu lieu.
- Le programme de bug bounty comprend trois domaines :
  - Recherche d'erreurs dans la documentation ou le code source qui ont été publiés (test statique).
  - Recherche d'erreurs par l'analyse du système opérationnel dans sa propre infrastructure (test dynamique).
  - Attaques contre l'infrastructure du fournisseur (test Internet), l'objectif de ce test étant exclusivement de pénétrer dans l'infrastructure. Il est possible d'exclure du programme de bug bounty les attaques par déni de service et les attaques d'ingénierie sociale. Dans les cas justifiés, il est permis d'interdire les attaques dirigées contre l'infrastructure (par ex. durant un scrutin).

Compétences et traitement des signalements :

- Le fournisseur du système est responsable du programme de bug bounty. Il assure le bon fonctionnement du programme, il réceptionne les signalements et il les classe par catégorie. Il communique ses décisions aux participants en les motivant et il publie tous les signalements de défaut qui sont confirmés. Il prend par ailleurs les mesures nécessaires pour corriger les défauts en question.
- La ChF fixe les conditions générales fondamentales régissant le programme de bug bounty.
- La Confédération et les cantons se voient accorder un accès illimité aux signalements ainsi qu'aux réponses du fournisseur du système. Dans le cadre de la procédure d'autorisation, une synthèse des signalements et des mesures prises sur la base de ces signalements doit être fournie.

Les conditions d'utilisation doivent être aménagées comme suit :

- La participation peut être anonyme; la révélation de l'identité d'une personne ne peut être demandée que dans la perspective du versement d'une indemnité dans le cadre d'un programme de bug bounty.
- Les participants sont autorisés à effectuer des publications concernant des défauts ou des défauts présumés. Le respect d'un délai en la matière peut être exigé (voir ci-après).
- Dans le souci de garantir une divulgation responsable (responsible disclosure), les participants peuvent être invités à respecter les règles suivantes :
  - Signaler immédiatement les défauts.
  - Attendre avant de signaler publiquement un défaut ; à cet égard, la ChF, les cantons et le fournisseur du système doivent fixer un embargo qui doit être respecté.
  - Adopter une attitude responsable à propos des informations concernant des défauts présumés. Ne pas diffuser inutilement des informations concernant des failles de sécurité potentielles. Les informations en la matière ne doivent être partagées et discutées qu'avec des personnes que l'on suppose aptes et disposées à traiter les questions en la matière, et qui adopteront elles aussi une attitude responsable.
  - Les violations de la « responsible disclosure » ne devraient pas être sanctionnées. Cette limitation de responsabilité est mentionnée dans les conditions d'utilisation.
- À propos du test Internet Le consentement du fournisseur du système au test protège les participants de toute poursuite pénale pour autant que les attaques menées ne soient pas exclues du test.

Avant la reprise des essais, la ChF adaptera les bases légales, en concertation avec les cantons, pour prévoir la mise en place d'un programme de bug bounty. En concertation avec les cantons et le fournisseur du système, elle fixera dans un catalogue d'exigences les conditions générales fondamentales qui régiront le programme de bug bounty. Il s'agira d'examiner une possibilité de processus de réclamation pour les participants qui ne seraient pas d'accord avec la décision du fournisseur du système.

Pour la reprise des essais, le test Internet doit être effectué sur le système productif. Ensuite, une décision sur la suite de la procédure peut être prise sur la base de l'expérience acquise. Il existe deux options : le test Internet peut être effectué de manière répétée sur le système productif ou comme un test continu sur un système jumeau.

Dialogue avec les milieux scientifiques

Les experts accordent une grande importance au contrôle public. Les défauts doivent être mis au jour, et les communications faites par le grand public doivent recevoir des réponses. Les experts recommandent la mise en place d'un programme permanent de bug bounty assorti d'un système d'indemnités financières. Le programme de bug bounty ne devra pas se limiter aux attaques réussies menées contre l'infrastructure du fournisseur du système; il devra aussi inclure les erreurs figurant dans la documentation relative au système et dans le code source. Les attaques contre l'infrastructure back-end du fournisseur du système, les intrusions physiques, les attaques par déni de service et les attaques d'ingénierie sociale ne doivent pas faire partie du champ d'application du programme de bug bounty, mais être testées par exemple dans le cadre de tests de pénétration confiés à des mandataires. L'établissement des objectifs et des modalités ainsi que la haute surveillance sont considérés comme étant du ressort de la Confédération ou d'un comité indépendant.

Impact de la mesure et appréciation globale du CoPil VE

Un programme de recherche des erreurs peut contribuer à améliorer en continu le système. Le programme de bug bounty renforcera le contrôle public, ce qui peut concourir à la mise en place d'une communauté de spécialistes et au renforcement de la confiance du public.

La ChF définit le cadre du programme de bug bounty. La définition des détails tels que le traitement des signalements individuels et le montant de la compensation financière est laissée aux fournisseurs de systèmes jusqu'à nouvel ordre. Elle se fera en concertation avec le NCSC, la ChF et les cantons. Il faut veiller à ce qu'une indemnisation et un traitement efficaces et crédibles des défauts signalés soient assurés.

- Estimation des coûts des variantes pour la poursuite ultérieure du test Internet (sans compensation financière) : Programme de bug bounty avec recherche d'erreur (test statique et dynamique) assorti d'un test Internet continu :
  - Coûts uniques : de 230 000 à 290 000 francs
  - Coûts récurrents (en moyenne) : de 55 000 à 70 000 francs par an
- Programme de bug bounty avec recherche d'erreur (test statique et dynamique) assorti d'un test Internet en continu :
  - Coûts uniques : de 255 000 à 360 000 francs
  - Coûts récurrents (en moyenne) : de 550 000 à 650 000 francs par an

De l'avis de la ChF, les coûts doivent être supportés avant tout par les cantons. Il s'agit d'examiner la possibilité d'un cofinancement par la Confédération de la gestion du programme, tout comme les modalités de participation d'autres services fédéraux.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
C.4	Publication des rapports d'audit pertinents pour l'autorisation	Reprise des essais	ChF, cantons, fournisseur

Objectif et description de la mesure

La Confédération, les cantons et le fournisseur du système œuvrent à la transparence à l'égard du public en ce qui concerne les résultats des audits en lien avec la procédure d'autorisation, ce qui permettra

aux milieux spécialisés d'effectuer un contrôle, et ce qui facilitera l'établissement de la confiance et la constitution d'une communauté de spécialistes. Cette mesure réglera les aspects suivants :

- Les rapports, certificats et justificatifs qui doivent être fournis dans le cadre des contrôles visés au ch. 5 de l'annexe de l'OVotE doivent être publiés. La responsabilité de la publication incombera à chaque entité commandant un rapport d'audit.
- Les rapports d'audit publiés doivent être compréhensibles. S'il y est fait référence à d'autres documents, ces derniers doivent également être publiés en règle générale. Si des documents supplémentaires ne peuvent pas être publiés, l'intelligibilité des rapports d'audit doit être garantie par la publication d'un résumé des éléments pertinents figurant dans les documents non publiés.
- Il peut être renoncé à la publication des rapports d'audit ou d'autres documents dans des cas justifiés, par exemple si la publication fait augmenter un risque, ou si des raisons de protection des données ou des directives de sécurité internes s'opposent à la publication.
- Les réponses que l'organisme contrôlé prépare en relation avec les rapports d'audit publiés doivent également être publiées.

La ChF adaptera les bases légales avant la reprise des essais.

Dialogue avec les milieux scientifiques

Les experts sont unanimes pour dire que la transparence est la condition sine qua non de tout contrôle public efficace. Ils sont une majorité à recommander la publication des rapports d'audit. À cet égard, il conviendra toutefois de veiller à la qualité élevée et à l'intelligibilité de ces rapports, faute de quoi leur publication pourrait entraîner une perte de confiance.

Impact de la mesure et appréciation globale du CoPil VE

Il est important d'établir une plus grande transparence à propos des rapports d'audit en rapport avec la procédure d'autorisation. Les publications s'adressent avant tout aux milieux spécialisés, et, dans une moindre mesure, au grand public. Il est important de tenir compte de la publication prévue des rapports d'audit durant l'intégralité du processus destiné à mandater des experts. La question de la publication doit être abordée avec les titulaires des mandats au moment où lesdits mandats sont attribués. La mise en œuvre de cette mesure aura dans tous les cas de faibles incidences financières pour le mandant, à savoir avant tout la Confédération.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
C.5	Lors des scrutins fédéraux, publication du résultat des votes exprimés à travers le vote électronique	Reprise des essais	Exigences : ChF Publication : Cantons

Objectif et description de la mesure

Il s'agit d'établir la transparence à l'égard du public à propos des résultats des votes exprimés par voie électronique. Les cantons doivent dès lors publier les résultats des élections et des votations fédérales pour le canal de vote électronique, ce qui permettra à la population de comparer les résultats du vote électronique avec le résultat global, d'effectuer un contrôle de plausibilité et d'asseoir sa confiance dans le vote électronique. Par ailleurs, la publication des résultats du vote électronique fournit des données et des informations qui peuvent constituer un fondement intéressant pour des travaux de recherche.

La ChF adaptera l'OVotE et fixera l'obligation de publier les résultats du vote électronique jusqu'à l'échelon communal. Elle prévoira à cet égard des exceptions afin que le secret du vote soit garanti dans tous les cas.

Dialogue avec les milieux scientifiques

La majorité des experts se sont prononcés en faveur de la publication des résultats du vote électronique. Les raisons principales de ce choix sont la transparence et la confiance. Certains experts ont aussi indiqué que la publication des résultats peut aboutir, indirectement, à la découverte de failles dans le système. Le secret du vote et la protection des données doivent être garantis en cas de publication.

Impact de la mesure et appréciation globale du CoPil VE

Les résultats du vote électronique doivent être publiés. S'agissant du degré de détail de la publication, les cantons ont fait remarquer qu'une publication à l'échelon communal pourrait se révéler problématique. Il conviendra de prévoir des exceptions dans les bases légales afin que la publication ne viole pas le secret du vote.

La mise en œuvre de cette mesure n'aura aucune incidence financière pour la Confédération, tandis que les incidences financières pour les cantons sont jugées minimes.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
C.6	Une participation accrue du public	Concept : reprise des essais	ChF avec la participation des cantons et fournisseur

Objectif et description de la mesure

Il convient d'impliquer davantage le public dans le vote électronique. Plusieurs mesures proposées dans le cadre de la restructuration promouvront la transparence et la constitution d'une communauté de spécialistes. En plus de ces mesures, la Confédération, les cantons et le fournisseur du système devront élaborer un concept pour renforcer la participation du public. Ce concept devra inclure des plans de communication active. Il s'agira de garantir la pérennité de la mise en œuvre de manifestations et de mesures d'information. Il s'agira également de mettre l'accent non seulement sur les décideurs politiques, les experts et les groupes d'intérêt, mais aussi sur le grand public. Pour ce faire, on pourra prévoir notamment les actions suivantes :

- Organiser des réunions d'information et de discussion ou participer à des réunions de ce type (conférences destinées aux décideurs politiques, aux partis, aux associations et à la communauté scientifique ; conférence E-Vote-ID à Bregenz).
- Lancer des concours d'idées (par ex. consacrés à des attaques d'ingénierie sociale) et organiser des hackathons.
- Exploiter une plateforme d'information.

Il s'agira d'élaborer une première version de ce concept avant la reprise des essais. La ChF en assumera la responsabilité. Les actions prévues seront mises en œuvre en continu. Les premières le seront si possible avant la reprise des essais. À titre d'exemple, le canton de Saint-Gall a déjà initié une plateforme d'information générale où les personnes intéressées peuvent se procurer des informations de fond sur le vote électronique. La plateforme est en cours de développement.

Dialogue avec les milieux scientifiques

D'une manière générale, les experts estiment que la communication et la transparence vis-à-vis du public sont deux éléments importants. À cet égard, il convient d'établir une distinction entre les milieux spécialisés et le grand public. Les manifestations à caractère technique, par exemple les hackathons et les concours d'idées, sont jugées judicieuses pour susciter l'intérêt des milieux spécialisés pour le vote électronique et pour les y associer. Pour le grand public, il faut trouver une approche qui favorise la compréhension du vote électronique et la confiance dans ce canal de vote. Les experts ont mentionné à cet égard les projets consacrés aux sciences participatives ainsi que les ateliers afin d'associer le grand public.

Impact de la mesure et appréciation globale du CoPil VE

Le renforcement de la communication et de la transparence vis-à-vis du grand public, du monde politique et des groupes d'intérêt, mais aussi la constitution d'une communauté de spécialistes, revêtent une grande importance. L'élaboration d'un concept aura peu d'incidences financières pour la Confédération et n'aura aucune incidence financière pour les cantons. La mise en œuvre des projets pourrait engendrer des coûts à la charge de la Confédération et des cantons.

D. Renforcement des liens avec les milieux scientifiques

N°	Mesure	Calendrier mise en œuvre	Responsabilité
D.1	Elaboration d'un concept pour le soutien scientifique des essais et le dialogue avec des experts externes	Concept : 2021	ChF avec la participation des cantons

Objectif et description de la mesure

Les essais de vote électronique feront l'objet d'une étude et d'un suivi scientifiques permanents. En outre, la Confédération et les cantons entretiendront un dialogue permanent avec la communauté scientifique et les services spécialisés compétents. Ils poseront des questions, répondront à des suggestions, participeront activement aux discussions et fourniront l'infrastructure et les ressources nécessaires aux échanges. La Confédération et les cantons commanderont par ailleurs des études scientifiques sur des sujets exigeant des recherches plus approfondies.

La Confédération et les cantons élaboreront en collaboration avec les représentants de la communauté scientifique un concept pour le suivi scientifique et le dialogue avec des experts externes pour la période 2022-2025, ainsi que pour le financement. Le développement de ce concept sera placé sous la responsabilité de la ChF.

Dialogue avec les milieux scientifiques

Les experts soulignent qu'un dialogue et une collaboration permanents entre les autorités et les milieux scientifiques sont essentiels au développement du vote électronique. Ils préconisent en particulier d'associer des experts indépendants à la conception et au développement du système, aux contrôles publics et commandés et à l'évaluation des risques, de promouvoir la recherche et de mettre sur pied de manière générale une communauté de spécialistes. Dans le dialogue avec les experts scientifiques, il s'agira de traiter non seulement les questions techniques, mais aussi, et de plus en plus, de thématiques relevant des sciences sociales. Pour permettre une vision globale et donc améliorer la sécurité des votations et des élections dans leur ensemble, la discussion sur la sécurité devra porter non seulement sur le vote électronique mais aussi sur les autres canaux de vote.

Impact de la mesure et appréciation globale du CoPil VE

Un suivi scientifique permanent est d'une importance capitale pour garantir la sécurité et un développement scientifique du vote électronique. Il s'agira de préciser les objectifs et les attentes vis-à-vis de ce suivi scientifique au moment de l'élaboration du concept. Il faudra notamment définir les responsabilités de la Confédération et des cantons ainsi que le financement de ce suivi. L'élaboration du concept aura peu d'incidences financières pour la Confédération et les cantons. La mise en œuvre du concept aura des implications financières en fonction de la forme sous laquelle il sera implémenté.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
D.2	Participation d'experts indépendants	Dans le cadre des mesures individuelles	ChF avec la participation des cantons

Objectif et description de la mesure

La Confédération et les cantons devraient associer à leurs travaux des experts ou services spécialisés indépendants actifs dans les disciplines scientifiques concernées, ainsi que d'autres organisations si cela devait se révéler utile et apporter une plus-value, en particulier pour les mesures définies dans le cadre de la restructuration :

- Définition et commande d'audits indépendants par la ChF
- Conception et mise en œuvre du service de vote électronique et des processus associés par les cantons et leurs partenaires
- Évaluation des demandes d'autorisation et notamment des résultats d'audits
- Examen des exigences fédérales en matière de sécurité
- Développement de concepts pour des mesures d'amélioration et leur inclusion dans le plan de mesures
- Préparation des bases pour les appréciations des risques

- Évaluation de risques individuels
- Élaboration de mesures visant à impliquer des experts indépendants
- Conduite d'ateliers ou de séminaires sur la convivialité et l'ergonomie
- Vérification du processus d'impression distribué

Les modalités selon lesquelles ces experts et services seront associés aux travaux seront discutées en relation avec les domaines de responsabilité respectifs. On examinera également l'opportunité de s'assurer pour certaines tâches le concours des services fédéraux compétents.

Dialogue avec les milieux scientifiques

Voir les commentaires sur les différentes mesures et sur la mesure D.1.

Impact de la mesure et appréciation globale du CoPil VE

Voir les commentaires sur les mesures individuelles et sur la mesure D.1. Cette mesure n'aura essentiellement d'incidences financières ni pour la Confédération ni pour les cantons. Les conséquences sont indiquées dans le cadre des mesures individuelles.

N°	Mesure	Calendrier mise en œuvre	Responsabilité
D.3	Elaboration d'un concept pour la mise en place d'un comité scientifique	Concept : 2022	ChF avec la participation des cantons

Objectif et description de la mesure

Un comité scientifique sera mis sur pied afin de conseiller la Confédération et les cantons. Ce comité devrait assumer des tâches de conseil dans la perspective d'une collaboration avec la communauté scientifique (au sens des mesures D.1 et D.2) et devrait également être en mesure d'accomplir lui-même certaines tâches. Il conviendra d'examiner comment ce comité pourra être intégré dans les processus actuels d'évaluation des systèmes, et s'il ne devrait pas assumer aussi une fonction de soutien aux cantons. Il faudra enfin définir les tâches et la composition du comité. La Confédération et les cantons élaboreront à cette fin un concept pour les années 2022 à 2025, sous la direction de la ChF.

Dialogue avec les milieux scientifiques

En plus des observations formulées sous la mesure D.1, les experts préconisent la création d'un comité scientifique chargé de conseiller les autorités. Ce comité assumerait une fonction de surveillance, mais pas de tâches réglementaires. En plus de ce comité scientifique, il a été proposé de mettre sur pied un conseil consultatif des citoyens qui pourrait par exemple assumer des tâches dans les domaines de l'information du public, du renforcement de la confiance du public et de la convivialité.

Impact de la mesure et appréciation globale du CoPil VE

Au-delà du suivi scientifique en général des essais, un conseil scientifique qui serait chargé de conseiller la Confédération et les cantons est préconisé. Il s'agira, lors de l'élaboration du concept, de déterminer les tâches de ce conseil consultatif et de régler les questions d'une éventuelle compensation financière et de la responsabilité du financement. L'élaboration du concept n'aura d'incidences financières ni pour la Confédération ni pour les cantons.

4. Évaluation globale et marche à suivre

4.1 Résumé des orientations et échelonnement des mesures

La mise en œuvre des mesures proposées doit répondre au besoin d'action identifié pour la reprise des essais et à moyen et long terme. Un processus d'amélioration continue sera nécessaire pour garantir la qualité et la sécurité des systèmes, l'efficacité des contrôles et des processus et pour renforcer la confiance dans le canal de vote électronique. Il conviendra à cet égard d'intensifier le dialogue avec la communauté scientifique et d'associer aux travaux davantage d'experts indépendants et le public. La reprise des essais suppose que différentes mesures soient mises en œuvre et que les bases légales soient adaptées. Il s'agira de mettre en œuvre une première phase d'améliorations, tout en continuant de travailler à la réalisation des objectifs de moyen et long terme. Les principales orientations proposées dans le catalogue de mesures peuvent être résumées comme suit :

Poursuite du développement des systèmes

– Assurer la qualité du système grâce à des spécifications plus précises des critères de qualité et à des processus traçables de développement et de déploiement	Reprise des essais ; processus d'amélioration continue
– Assurer la *forensic readiness* des systèmes utilisés au moyen d'une détection et d'une investigation efficaces des incidents	Reprise des essais ; processus d'amélioration continue
– Créer un instrument de planification commun et public de la Confédération et des cantons pour la mise en œuvre continue des mesures de sécurité	Reprise des essais ; audit continu
– Renforcer la vérifiabilité par une plus grande diversité et une plus grande indépendance des différents composants	À moyen terme ; travaux d'approfondissement jusqu'à 2 ans après la reprise des essais

Surveillance et contrôle efficaces

– Assurer l'efficacité des audits indépendants du système	Reprise des essais
– Mettre en place une procédure réglementée pour le traitement des non-conformités avérées ou présumées	Reprise des essais
– Améliorer l'appréciation des risques et la gestion de crise	Reprise des essais ; processus d'amélioration continue
– Poursuivre le développement des contrôles de plausibilité	En continu, première étape jusqu'en 2022
– Procéder à des ajustements et au contrôle des processus dans la procédure d'approbation, ainsi que des processus, rôles et tâches	Reprise des essais et audit à long terme

Renforcement de la transparence et de la confiance

– Limitation de l'électorat en phase d'essai	Reprise des essais
– Assurer plus de transparence et un accès plus facile aux informations sur le système, aux rapports d'audit et aux résultats	En continu
– Mettre sur pied et veiller à une participation accrue d'une communauté composée d'experts et du public (décideurs politiques, milieux spécialisés, groupes d'intérêt et grand public) en vue d'un contrôle public continu	

Renforcement des liens avec les milieux scientifiques

– Assurer un suivi continu par la communauté scientifique et associer aux travaux des experts indépendants	Thème transversal, mise en œuvre continue
– Mettre en place un comité scientifique chargé d'assister et de conseiller la Confédération et les cantons	À moyen terme

4.2 Conséquences pour la Confédération et les cantons

4.2.1 Mesures en vue de la reprise des essais et des premières étapes après la reprise des essais

Certaines des mesures pour la reprise des essais n'auront pas ou n'auront que peu de conséquences directes en termes de coûts pour la Confédération et les cantons. On peut supposer que ces coûts pourront être couverts par la Confédération et les cantons selon leurs compétences. Les mesures suivantes, toutefois, qui sont également prévues pour la reprise des essais ou les premières étapes après la reprise des essais, auront un impact financier plus important :

- *Verifier* et composants de contrôle indépendants du fournisseur (mesure A.4) : la mise en œuvre de la première étape (établissement d'une étude sur les composants de contrôle en ligne indépendant) devrait probablement entraîner pour les cantons des coûts faibles à moyens.
- Réduction des hypothèses de confiance dans le processus d'impression (mesure A.5) : selon une première estimation des coûts, l'adaptation du protocole cryptographique entraîne des coûts élevés au cours de la première phase[19]. Selon la répartition actuelle des compétences, ces coûts devraient être supportés par les cantons. Or, les cantons ne pouvant faire face à cette charge à eux seuls, il faudra envisager un cofinancement par la Confédération.
- Tableau d'affichage public (mesure A.6) : selon une première estimation, la mise en œuvre de la première étape (établissement d'une étude) devrait probablement entraîner pour la Confédération des coûts moyens.
- Audit indépendant des systèmes (mesure B.1) : cette mesure a un impact financier élevé pour la Confédération, qui sera à l'avenir responsable de ces audits, exception faite de la certification ISO27001 du fournisseur du système, qui les commandera à l'extérieur et qui en supportera donc les coûts. La mise en œuvre des audits indépendants pourra probablement être financée par la Confédération, à condition que les fonds nécessaires soient approuvés.
- Gestion d'un programme permanent de *bug bounty* (mesure C.3) : selon une première estimation des coûts effectuée par La Poste, la mise en œuvre entraîne des coûts moyens à élevés, selon la conception retenue[20]. En outre, la compensation financière des signalements occasionnera elle aussi certains coûts. Selon la répartition actuelle des compétences, ces coûts devraient être supportés par les cantons. Or, les cantons ne pouvant faire face à cette charge à eux seuls, il faudra envisager un cofinancement par la Confédération.

4.2.2 Développements de moyen à long terme

Les mesures sont importantes pour la sécurité et la fiabilité du vote électronique et conditionnent donc son avenir.

Le financement des développements de moyen à long terme n'est pas assuré. Il est particulièrement critique pour les trois mesures suivantes. En effet, si ces mesures prévoient dans un premier temps la réalisation d'études et de travaux d'approfondissement qui devraient entraîner des coûts faibles à moyens, la mise en œuvre ultérieure devrait par contre être très coûteuse :

- *Verifier* et composants de contrôle indépendants du fournisseur (mesure A.4) : Les coûts occasionnées par le recours à des composants en ligne indépendants du fournisseur sont très importants et, selon la répartition actuelle des compétences, devraient être supportés par les cantons. Or, les cantons ne pouvant faire face à cette charge à eux seuls[21], il faudra envisager un cofinancement par la Confédération.

[19] Coûts uniques compris entre 850 000 et 1 million de francs.

[20] Estimation des coûts pour le programme de *bug bounty* avec test Internet périodique : coûts uniques de 230 000 à 290 000 francs et coûts récurrents de 55 000 à 70 000 francs par an. Programme de *bug bounty* avec test Internet en continu : coûts uniques de 255 000 à 360 000 francs et coûts récurrents de 550 000 à 650 000 francs par an.

[21] Composants de contrôle : coûts uniques de 1,8 à 2,2 millions de francs et coûts récurrents de 600 000 à 800 000 francs par an. *Verifier* : coûts uniques de 0,9 à 1 million de francs et coûts récurrents de 200 000 francs par an.

- Réduction des hypothèses de confiance dans le processus d'impression (mesure A.5) : les coûts de mise en œuvre sont importants et, selon la répartition actuelle des compétences, devraient être supportés par les cantons. Or, les cantons ne pouvant faire face à cette charge à eux seuls[22], il faudra envisager un cofinancement par la Confédération.
- Tableau d'affichage public (mesure A.6) : selon une première estimation, l'éventuelle mise en œuvre de cette mesure entraînerait des coûts élevés[23]. Il faut encore éclaircir la question de la responsabilité du financement.

4.2.3 Sécurisation à long terme du financement

Possibilités de financement

Garantir la sécurité du vote électronique entraînera des coûts élevés et ces coûts devraient être plus élevés à l'avenir. Or, le financement devra être garanti à long terme. Si les cantons ne peuvent supporter les coûts de mesures importantes sur le plan matériel, il faudra examiner de nouvelles possibilités de financement.

Il s'agira d'explorer les possibilités de financement suivantes :

- Le plan de mise en œuvre de eGovernment Suisse prévoit d'allouer annuellement 250 000 francs au vote électronique jusqu'en 2023. Ces fonds permettraient de financer certains projets et études spécifiques, mais ne suffiraient pas pour couvrir les développements à moyen et long terme. Aussi convient-il d'examiner s'il serait possible de les augmenter et s'il serait ainsi possible de financer certains projets par des moyens supplémentaires accordés à eGovernment Suisse.
- Il faudra examiner la possibilité de trouver de nouvelles sources de financement auprès des cantons.
- Il faudra examiner la possibilité de trouver de nouvelles sources de financement auprès de la Confédération.

Il s'agira en outre de créer autant que possible dans la mise en œuvre des mesures des synergies entre tous les acteurs concernés. Cela suppose d'intensifier la collaboration avec les structures déjà existantes et de se demander par exemple comment exploiter au mieux les ressources du Centre national pour la cybersécurité (NCSC) et les interfaces avec les processus existants au sein de la ChF, des cantons et de La Poste.

Évaluation par les cantons

Pour les cantons, il est clair que seuls des systèmes sécurisés de vote électronique doivent être implémentés. Les cantons disposent a priori d'une marge de manœuvre limitée en ce qui concerne le financement du vote électronique. Dans nombre d'entre eux, la pression politique sur les ressources prévues pour le vote électronique s'est accrue et risque de s'accentuer encore si le vote électronique ne peut faire l'objet d'une utilisation productive pendant une période prolongée. Aussi les cantons estiment-ils qu'il serait irréaliste de demander des moyens supplémentaires. D'autre part, seuls quelques rares cantons seront en mesure dans les années à venir de proposer le vote électronique. Or, le poids du financement des mesures arrêtées dans le cadre de la restructuration ne pourra reposer tout entier sur les épaules de ces cantons.

Les cantons ont certes été en mesure d'assumer les coûts jusqu'à présent, mais on peut supposer que La Poste répercutera sur eux la mise en œuvre des nouvelles exigences. Pour les cantons, ce qui importe, c'est le prix par électeur. Aussi les coûts supplémentaires encourus par La Poste ne pourront-ils être couverts que par un élargissement de l'électorat admis à prendre part au vote électronique et par une augmentation des cantons participants.

La décision quant à la mise en œuvre des mesures doit tenir compte de la marge de manœuvre limitée dont disposent les cantons en matière de financement. La question du financement doit être l'un des facteurs déterminants pour décider de la mise en œuvre ou non d'une mesure. S'agissant des mesures

[22] Coûts uniques de 700 000 à 900 000 francs et coûts récurrents de 100 000 francs par an.

[23] Coûts uniques de 600 000 francs et coûts récurrents de 200 000 francs par an.

que les cantons ne sont pas en mesure de financer, il conviendra de rechercher des sources de financement alternatives. Il faudra vérifier dans quelle mesure la Confédération pourra contribuer à ce financement.

Evaluation de la ChF

Garantir la sécurité est essentiel à l'utilisation d'un canal de vote électronique digne de confiance. Ce faisant, les autorités et les fournisseurs de systèmes seront davantage confrontés à des coûts élevés. Cependant, du point de vue de la ChF, ce sont précisément les mesures qui impliquent des coûts élevés qui apportent un gain considérable en matière de sécurité. En particulier le « *Public Scrutiny* », la participation de la communauté scientifique et le renforcement de la sécurité et de la vérifiabilité sur la base de résultats scientifiques offrent une grande valeur ajoutée selon la ChF. La mise en œuvre de ces mesures est donc essentielle pour le développement du vote électronique. Cette évaluation correspond également aux résultats du dialogue avec les milieux scientifiques. Puisque le financement de ces mesures ne peut être garanti avec les budgets fédéraux et cantonaux actuels, de nouvelles solutions de financement doivent être recherchées. Du point de vue de la ChF, il est important que la Confédération et les cantons s'efforcent de mettre en œuvre ces mesures et qu'ils s'engagent dès à présent à assurer le financement nécessaire.

5. Conclusions

Afin de remplir les objectifs définis par le Conseil fédéral pour la restructuration de la phase d'essai, le CoPil VE a adopté un catalogue de mesures avec le présent rapport final. Ce catalogue de mesures définit les orientations à court, moyen et long terme des travaux de la Confédération et des cantons pour les années à venir, y compris un horizon temporel pour la mise en œuvre et un partage des responsabilités. L'accent est mis sur un processus d'amélioration continue et non plus sur un label de qualité incarné par la certification. La sécurité, la confiance et l'acceptation du vote électronique devraient être continuellement renforcées avec la participation d'experts des milieux scientifiques et de l'industrie. La Confédération et les cantons doivent examiner en continu les mesures nécessaires et les adapter au besoin.

Dans un premier temps, il s'agira de mettre en œuvre les mesures prévues pour la reprise des essais et d'adapter en conséquence les bases légales, ce qui permettra aux cantons de reprendre rapidement les essais. Parallèlement à la reprise des essais avec un électorat limité, des travaux seront menés en vue de mettre en œuvre les mesures à moyen et long terme. La poursuite des essais dans certains cantons permettra d'éviter que les cantons et La Poste, en tant que fournisseur du système, ne perdent les ressources et le savoir-faire existants ainsi que les investissements déjà réalisés. Elle permettra également à tous les acteurs concernés d'acquérir une expérience précieuse dans l'utilisation des systèmes entièrement vérifiables. Plusieurs mesures telles que le maintien de la limitation de l'électorat souligneront le caractère expérimental du projet. Par ailleurs, le principe qui veut que « la sécurité prime la vitesse » continuera de s'appliquer. Dans un second temps, seront menés des travaux en vue de mettre en œuvre les mesures à moyen et long terme.

Garantir la sécurité des systèmes utilisés est une priorité absolue. Les mesures de restructuration prévoient une définition plus précise des exigences de sécurité, un contrôle et une surveillance plus efficaces avec l'implication des milieux scientifiques ainsi qu'une amélioration de la gestion des risques. La Confédération et les cantons veulent renforcer en outre la confiance dans le vote électronique en créant une plus grande transparence et en cherchant à collaborer plus étroitement avec le public et les milieux scientifiques. La communauté actuelle de spécialistes du vote électronique devra être élargie, avec un rôle important dévolu aux scientifiques. Des experts indépendants seront associés davantage à l'élaboration des informations de base, au suivi des essais et notamment à l'audit des systèmes. La possibilité de procéder à des audits publics sera elle aussi renforcée. Les informations concernant le système utilisé (en particulier la documentation et le code source) seront publiées, ainsi les documents nécessaires pour le contrôle seront mis à disposition du public. Les rapports d'audit et les résultats du canal de vote électronique seront publiés, ce qui permettra aux électeurs et aux experts de se faire leur propre opinion et de fournir un retour d'information aux autorités à tout moment. Ces retours d'information serviront à développer et à améliorer en continu le vote électronique.

Une communication transparente vis-à-vis du public joue un rôle important dans le renforcement de la confiance dans le canal de vote électronique. La Confédération et les cantons doivent informer le public sur les questions de sécurité, ce qui constitue une tâche importante s'agissant de sujets techniquement aussi complexes que le vote électronique. Aussi la Confédération et les cantons veulent-ils renforcer la communication et l'information du public et mettre en œuvre les mesures nécessaires.

Il est essentiel que la situation de départ pour l'utilisation du vote électronique soit évaluée en permanence à la lumière des développements les plus récents. La mise en œuvre de différentes mesures et l'adaptation des bases légales doivent permettre de poursuivre la phase d'essai du vote électronique. Développer et améliorer sans cesse est important pour assurer la sécurité et la fiabilité du vote électronique. Mais ce travail de développement et d'amélioration en continu dépend d'un financement garanti à long terme. Or, tel n'est pas le cas avec les moyens aujourd'hui prévus par la Confédération et les cantons. Aussi la Confédération et les cantons devraient-ils rechercher de nouvelles sources de financement.

Annexe: Catalogue des mesures

Nr.	Mesure	Description	Calendrier mise en œuvre	Responsabilité	Appréciation des coûts[24] *Bas (<50'000 CHF)* *Moyen (50'000 - 500'000 CHF)* *Elevé (500'000 - 1 Mio. CHF)* *Très élevé (> 1 Mio. CHF)*
A.	**Poursuite du développement des systèmes**				
A.1	Précision des critères qualité pour le code source et la documentation y relative	Les critères de qualité qui s'appliquent aujourd'hui au code source et à sa documentation seront précisés. Des critères clairs devront garantir une qualité élevée des systèmes de vote électronique. En outre, les audits de tous les acteurs et du public devront être facilités. Ces critères seront ensuite utilisés dans les processus d'assurance qualité liés au développement des logiciels.	Reprise des essais	Exigences : ChF Mise en œuvre : Cantons, fournisseur du système	Confédération : aucun Cantons : aucun
A.2	Renforcement de l'assurance qualité dans le processus de développement du système	Les exigences vis-à-vis des processus d'assurance qualité entourant le processus de développement du système doivent être précisées. De cette manière, les objectifs suivants devront être atteints : - Suivre et contrôler les modifications - Maintenir une traçabilité bidirectionnelle permanente entre les éléments de documentation (protocole, spécifications, architecture, etc.) et le code - Intégrer les résultats des processus de revue dans le développement - Assurer et maintenir la conformité aux exigences légales tout au long du cycle de vie	Reprise des essais	Exigences : ChF Mise en œuvre : Cantons, fournisseur du système	Confédération : aucun Cantons : aucun
A.3	Mise en œuvre d'une méthode éprouvée et vérifiable de construction et de déploiement	Les exigences à l'égard du fournisseur du système seront complétées afin qu'une méthode permettant la traçabilité de la construction du système à partir du code source jusqu'à son installation en production (construction et déploiement) soit appliquée. Les objectifs suivants devraient être atteints: - La méthode de construction et de déploiement du logiciel devra permettre de s'assurer que la version du logiciel déployé correspond bien à celle qui a été publiée, testée et autorisée. - En plus de cette traçabilité, elle devra empêcher dans la mesure du possible d'éventuelle manipulation des livrables. - Elle devra également prévenir l'introduction de vulnérabilités pertinentes pour le logiciel qui pourraient effectivement rendre le système vulnérable par les outils de développement et librairies utilisés.	Reprise des essais	Exigences : ChF Mise en œuvre : Cantons, fournisseur du système	Confédération : aucun Cantons : bas

[24] Les estimations des coûts supplémentaires (coûts externes ou ressources supplémentaires) supportés par la Confédération et les cantons sont présentés. Les coûts encourus par le fournisseur du système sont intégrés dans les coûts des cantons dans la mesure où ils sont répercutés.

Nr.	Mesure	Description	Calendrier mise en œuvre	Responsabilité	Appréciation des coûts[24] *Bas (<50'000 CHF)* *Moyen (50'000 - 500'000 CHF)* *Elevé (500'000 - 1 Mio. CHF)* *Très élevé (> 1 Mio. CHF)*
		Le processus de traitement des non-conformités (cf. mesure B.3) devra être activé dans le cas où une vulnérabilité devrait subsister.			
A.4	Utilisation de composants indépendants du fournisseur (« Verifier », composants contrôle)	La ChF et les cantons doivent approfondir les informations servant de base dans le domaine des composants indépendants du fournisseur. La priorité est donnée à l'élaboration des bases dans le domaine des composants de contrôle indépendants du fournisseur actifs dans la génération des codes de contrôle et la conservation des suffrages jusqu'au dépouillement (composants de contrôle en ligne). Le CoPil VE a l'intention d'utiliser des composants de contrôle en ligne indépendants du fournisseur dans un délai d'environ cinq ans après la reprise des essais. Cette déclaration d'intention est subordonnée à l'obtention d'un financement. Une masse critique de cantons actifs est nécessaire pour répartir les charges. En particulier, un nombre suffisant de cantons doit être disposé à supporter les coûts à la charge des cantons. Il en va de même avec la réserve qu'aucune raison importante inconnue à ce jour ne s'oppose à une mise en œuvre ultérieure. Dans un premier temps, une étude sera réalisée en vue de déterminer l'organisation et les responsabilités possibles pour l'attribution des contrats, la maintenance, l'exploitation et de régler les éventuelles questions techniques. En particulier, les effets sur les procédures opérationnelles des cantons et les coûts de mise en œuvre doivent être exposés. En outre, une proposition concrète de calendrier pour la mise en œuvre devra être abordée dans l'étude (selon une première évaluation des cantons, on peut s'attendre à un horizon d'au moins trois à cinq ans pour la mise en œuvre). L'étude doit servir de base à la décision de mise en œuvre. La préparation de l'étude relèvera de la responsabilité des cantons. Une fois l'étude est terminée, la ChF et les cantons soumettront une proposition au CoPil VE pour la suite de la procédure.	Etude et proposition composants de contrôle en ligne au CoPil VE : jusqu'à 2 ans après la reprise des essais Mise en œuvre sous réserve : environ 5 ans après la reprise des essais	Etude composants de contrôle en ligne : Cantons, avec la participation de la ChF	<u>Etude composants de contrôle en ligne</u> Confédération : aucun Cantons : bas - moyen <u>Estimation pour une éventuelle mise en œuvre après l'étude</u> Confédération : participation à évaluer Cantons : très élevé Composants contrôle : - Unique : 1.8-2.2 millions CHF - Récurrent : 0.6-0.8 million CHF / an Verifier : - Unique : 0.9 à 1 million CHF - Récurrent : 200'000 CHF / an
A.5	Réduction des hypothèses de confiance dans le processus d'impression et le logiciel qui génère les paramètres cryptographiques	Il est prévu de réduire les hypothèses de confiance admissibles dans le processus d'impression et le logiciel qui génère les paramètres cryptographiques. On s'assurera au moyen d'un logiciel indépendant du fournisseur que les paramètres cryptographiques et en particulier les codes de vérification ont été générés de manière aléatoire. Pour atteindre l'entropie souhaitée, quatre composants de contrôle au moins doivent être utilisés pour la génération de valeurs privées. Dans une évaluation par échantillonnage, il s'agira de vérifier des cartes de vote	Approfondissement et adaptation du protocole cryptographique : 1 an après la reprise des essais Proposition au CoPil VE :	Clarification des questions ouvertes concernant les exigences : ChF Mise en œuvre : Cantons	<u>Approfondissement et adaptation du protocole cryptographique</u> Confédération : bas ; participation à évaluer Cantons : élevé Adaptation du protocole cryptographique : 850'000-1 million CHF

Nr.	Mesure	Description	Calendrier mise en œuvre	Responsabilité	Appréciation des coûts[24] *Bas (<50'000 CHF)* *Moyen (50'000 - 500'000 CHF)* *Elevé (500'000 - 1 Mio. CHF)* *Très élevé (> 1 Mio. CHF)*
		prises au hasard afin de s'assurer que les valeurs imprimées correspondent bien aux valeurs vérifiées. Le CoPil VE a l'intention d'adapter la génération des paramètres ainsi que le processus d'impression dans un délai d'environ quatre ans après la reprise des essais. Cette déclaration d'intention est subordonnée à l'obtention d'un financement. Une masse critique de cantons actifs est nécessaire pour répartir les charges. En particulier, un nombre suffisant de cantons doit être disposé à supporter les coûts à la charge des cantons. Il en va de même avec la réserve qu'aucune raison importante inconnue à ce jour ne s'oppose à une mise en œuvre ultérieure. Dans un premier temps, la ChF et les cantons approfondiront la solution envisagée, et les cantons feront procéder à l'adaptation du protocole cryptographique. Ils définiront leurs processus en collaboration avec La Poste. Une première estimation du calendrier a montré que la mise en œuvre (y compris l'adaptation du protocole cryptographique) prendrait certainement trois ans. La planification de la mise en œuvre devra être approfondie dans le cadre de la première étape. Une fois achevés les travaux d'approfondissement, la ChF et les cantons soumettront au CoPil VE une proposition détaillée de mise en œuvre.	jusqu'à 2 ans après la reprise des essais Mise en œuvre sous réserve : environ 4 ans après la reprise des essais		<u>Estimation pour une éventuelle mise en œuvre après l'approfondissement</u> Confédération : participation à évaluer Cantons : élevé - Unique : 700'000-900'000 CHF - Récurrent : 100'000 CHF / an
A.6	Approfondissement des informations servant de base à l'introduction d'un mécanisme de vérifiabilité supplémentaire dont l'efficacité ne repose pas sur les hypothèses de confiance actuelles	Les possibilités de prévoir un mécanisme de vérifiabilité supplémentaire seront approfondies. Il conviendra ainsi d'examiner si et de quelle manière il serait possible de mettre à la disposition des électeurs un instrument de vérifiabilité qui s'ajouterait à ceux qui ont été fournis par le fabricant. Un tel mécanisme pourrait par exemple être mis en place sous la forme d'un tableau d'affichage public (*Public Bulletin Board*), qui permettrait de rendre publiques les données relatives au vote tout en respectant sa confidentialité et permettrait aux votants, à l'aide d'un second dispositif (p. ex. un téléphone portable), de vérifier si leur vote est bien parvenu sur une ou plusieurs instances indépendantes du fournisseur. De cette manière, l'efficacité de la vérifiabilité individuelle ne dépendrait pas de la fiabilité de l'imprimerie ou des composants de contrôle. Dans le cadre des vérifications faites au sens de la vérifiabilité universelle, les cantons pourraient s'assurer que tous les votes enregistrés par les instances indépendantes ont été pris en compte dans le dépouillement.	Etude : 1 an après la reprise des essais Proposition au CoPil VE : jusqu'à 2 ans après la reprise des essais	Etude : ChF avec la participation des cantons	<u>Etude</u> Confédération : moyen Cantons : aucun <u>Estimation pour une éventuelle mise en œuvre après l'approfondissement</u> Elevé. Le financement de la mise en œuvre est encore à clarifier. - Unique : 600'000 CHF - Récurrent : 200'000 CHF / an

Nr.	Mesure	Description	Calendrier mise en œuvre	Responsabilité	Appréciation des coûts[24] *Bas (<50'000 CHF)* *Moyen (50'000 - 500'000 CHF)* *Elevé (500'000 - 1 Mio. CHF)* *Très élevé (> 1 Mio. CHF)*
		Dans un premier temps, il s'agira de développer une étude afin d'approfondir l'utilité d'un mécanisme supplémentaire ainsi que la forme de sa mise en œuvre éventuelle. Cette étude devra aborder les questions relatives à la mise en œuvre technique et, avec la participation des votants, les questions de renforcement de la confiance et d'acceptabilité. Une fois ce travail préliminaire terminé, la ChF et les cantons soumettront au CoPil VE une proposition détaillée sur l'opportunité de mettre en place un tableau d'affichage public, et selon quelles modalités. Le financement devra être assuré en vue de la mise en œuvre.			
A.7	Amélioration des capacités de détection (monitoring) et d'investigation (investigation numérique) des incidents	Les systèmes de vote électronique doivent permettre de détecter et d'investiguer efficacement les incidents, tels que les soupçons de manipulation des votes ou les attaques contre le système. Les exigences actuelles en matière de collecte de traces seront précisées comme suit en vue de la reprise des essais : des logs cohérents seront établis à travers tous les éléments du système pour la détection et l'investigation des incidents ; ces logs devront être collectés, transférés et stockés d'une manière interdisant leur manipulation ; leur contenu devra être défini avec l'objectif de pouvoir conduire une investigation efficace des incidents. Le secret du vote doit être garanti. Dans un deuxième temps et dès la reprise des essais sera défini et mis en œuvre un processus d'amélioration en continu pour la détection et l'investigation des incidents. Il y aura lieu de tenir compte notamment des aspects suivants : - Un échange ouvert entre la Confédération, les cantons et les fournisseurs de systèmes - Une analyse régulière portant sur l'adéquation des systèmes de monitoring et d'investigation. Les scénarios définis dans la convention de crise sont pris en compte dans ces analyses. - La prise en compte des éléments résultant de l'analyse dans le cadre de l'amélioration des instruments et des processus	Définition des exigences et du processus d'amélioration : Reprise des essais	Exigences : ChF Processus d'amélioration : Fournisseur, cantons	Confédération : aucun Cantons : aucun ; la mise en œuvre continue des mesures issues du processus d'amélioration entraînera des coûts d'un montant inconnu
A.8	Création d'un plan d'action commun de la Confédération et des cantons	A l'avenir, la Confédération et les cantons mettront en œuvre un plan d'action commun. Le plan d'action reflète les décisions relatives à la restructuration de la phase d'essais et indique les mesures déjà mises en œuvre pour la reprise des essais et celles qui doivent être utilisées pour développer le vote électronique à moyen ou long terme. Lorsque cela est possible, il convient d'indiquer les délais de mise en œuvre des	Reprise des essais	ChF / cantons	Confédération : aucun Cantons : aucun

Nr.	Mesure	Description	Calendrier mise en œuvre	Responsabilité	Appréciation des coûts[24] *Bas (<50'000 CHF) Moyen (50'000 - 500'000 CHF) Elevé (500'000 - 1 Mio. CHF) Très élevé (> 1 Mio. CHF)*
		mesures ou les premières étapes prévues. Le CoPil VE adoptera le plan d'action sous la forme d'une déclaration d'intention et le publiera. Il sera revu régulièrement, afin de garantir le maintien de la sécurité compte tenu des dernières évolutions en la matière.			

B.	**Surveillance et contrôle efficaces**				
B.1	Modification des compétences dans le cadre de l'évaluation de la conformité du système et des processus qui l'entourent	Les responsabilités dans l'évaluation des systèmes seront révisées. L'efficacité et la crédibilité de l'audit sera ainsi assurée. L'indépendance entre l'organisme d'audit et l'entité auditée joue un rôle important à cet égard. La répartition des responsabilités entre la Confédération et les cantons sera adaptée de manière à ce que la Confédération assume plus de responsabilités et un rôle plus direct dans l'audit des systèmes : - La Confédération sera dès lors responsable des contrôles de conformité aux exigences du système et des processus qui l'entourent (chapitre 5.1, 5.2, 5.3 en partie et 5.4, 5.5 et 5.6 de l'annexe à l'OVotE) - A l'avenir, le fournisseur de système sera uniquement responsable des contrôles liés à l'exploitation du système dans ses centres de calcul (certification ISO 27001 prévue au chapitre 5.3 de l'annexe à l'OVotE) Des experts indépendants doivent être mandatés pour ces audits.	Reprise des essais	ChF	Confédération : élevé Cantons : aucun (pas de réduction des coûts)
B.2	Elaboration d'un concept d'audit pour l'évaluation de la conformité du système et des processus qui l'entourent	En se basant sur les responsabilités définies dans la mesure B.1, un concept d'audit sera établi. Le concept d'audit sera conçu de manière à garantir un passage en revue complet des exigences de sécurité. Cette tâche est de la responsabilité de la ChF. Elle peut toutefois recourir à des experts externes pour l'aider. Le concept devra prévoir entre autres : - Une définition claire de la portée des différents domaines d'examen tant du point de vue de leur périmètre que de leur durée de validité - Une perméabilité entre les différents domaines d'examen afin d'assurer un contrôle cohérent et complet - Mandat d'experts qualifiés et indépendants - La publication des rapports d'audit	Reprise des essais	ChF en collaboration avec les cantons et le fournisseur du système	Confédération : bas Cantons : aucun

Nr.	Mesure	Description	Calendrier mise en œuvre	Responsabilité	Appréciation des coûts[24] *Bas (<50'000 CHF)* *Moyen (50'000 - 500'000 CHF)* *Elevé (500'000 - 1 Mio. CHF)* *Très élevé (> 1 Mio. CHF)*
B.3	Elaboration et mise en œuvre d'un processus de traitement des non-conformités	La ChF élabore avec les cantons et le fournisseur de système un processus de traitement des non-conformités avérées ou présumées. La mise en place d'un processus de traitement des non-conformités vise à prévenir autant que possible les incertitudes face à une non-conformité et à garantir que l'utilisation du vote électronique se fera conformément aux exigences de l'OVotE. Ce processus devra définir : - Les types de non-conformité - Quels critères seront appliqués pour le traitement des non-conformités - Qui en seront les acteurs et avec quel rôle	Reprise des essais	ChF en collaboration avec les cantons et le fournisseur du système	Confédération : bas Cantons : aucun
B.4	Renouvellement et amélioration du guide pour l'appréciation des risques	La ChF, en collaboration avec les cantons, le fournisseur de système et des experts en sécurité informatique renouvelle le guide pour l'appréciation des risques qui servira de base aux appréciations des risques prévues dans la mesure B.5. Ce guide définit en particulier : - Un catalogue d'actifs informationnels (information assets) - Un catalogue de menaces basé sur celui de l'OVotE - Un catalogue de mesures de mitigation - Les responsabilités en matière de protection des actifs informationnels Le guide devra par ailleurs tenir compte de la longueur des clés de chiffrement, du vote multiple par différents canaux, de l'achat de votes, de la *long term privacy* et de la dépendance à l'égard d'un fournisseur unique. Le guide sera publié afin de renforcer la transparence et la confiance. En outre, il donnera ainsi la possibilité au public de donner son avis. Le guide devra être revu périodiquement et adapté au besoin.	Reprise des essais	ChF en collaboration avec les cantons et le fournisseur du système	Confédération : bas Cantons : aucun
B.5	Elaboration et mise en œuvre d'un nouveau processus d'appréciation des risques pour des systèmes complètement vérifiables	L'appréciation des risques sera effectuée par chaque acteur (ChF, cantons, fournisseurs de systèmes) selon ses responsabilités. Elle implémentera le guide défini dans la mesure B.4. Elle sera mise à jour et, le cas échéant, adaptées au moins une fois par année ainsi que lors de modifications fondamentales du système, spécialement avant chaque scrutin. Si les mesures de mitigation ne peuvent être mises en œuvre	Reprise des essais	ChF, cantons, fournisseur du système	Confédération : bas Cantons : bas

Nr.	Mesure	Description	Calendrier mise en œuvre	Responsabilité	Appréciation des coûts[24] *Bas (<50'000 CHF)* *Moyen (50'000 - 500'000 CHF)* *Elevé (500'000 - 1 Mio. CHF)* *Très élevé (> 1 Mio. CHF)*
		immédiatement, elles doivent être incluses dans le plan d'action (mesure A.8). Des experts indépendants seront impliqués dans l'évaluation des risques.			
B.6	Renouvellement de la gestion de crises avec conduite d'exercices de crise	Pour tenir compte des évolutions du vote électronique ainsi qu'améliorer l'efficacité de la gestion de crise, une nouvelle convention de crise doit être établie. Elle prendra la forme d'un contrat cadre et aura les propriétés suivantes : - Tripartite, conclue entre la ChF, les cantons utilisateurs d'un système et le fournisseur du système - Comprendre une définition des processus et des acteurs impliqués dans la gestion de crise - Comprendre les processus de communication entre les différentes parties prenantes ainsi que les processus de coordination en matière de communication externe - Prévoir la conduite d'exercices afin d'améliorer la gestion de crises. - La convention de crise adaptera les scénarios de crise aux appréciations des risques nouvellement applicables aux systèmes entièrement vérifiables. Les structures existantes mises en place par la Confédération, les cantons et les fournisseurs de systèmes seront maintenues autant que possible dans la gestion de crise.	Reprise des essais	ChF (lead), cantons et fournisseur du système	Confédération : bas Cantons : aucun
B.7	Intégration du vote électronique dans les infrastructures critiques de la Confédération	Les infrastructures critiques au sens de la Stratégie nationale pour la protection des infrastructures critiques jouissent d'un soutien particulier de MELANI et de GovCERT. Ce soutien serait précieux dans l'analyse des menaces et dans l'investigation d'incidents. Cette mesure vise à définir la coopération entre la ChF, les cantons, le fournisseur de système et GovCERT / MELANI en matière de vote électronique afin de garantir un accès prioritaire pour le traitement des incidents. Cette collaboration devrait également être prise en compte dans la gestion des crises.	Reprise des essais	ChF (lead), cantons et fournisseur du système	Confédération : aucun Cantons : aucun
B.8	Poursuite du développement du contrôle de la plausibilité des résultats du vote électronique	Les cantons contrôlent la plausibilité des résultats du vote électronique de manières diverses. Il s'agit donc d'intensifier les échanges entre les cantons et avec la ChF, de façon que les différentes expériences et approches puissent être discutées dans une perspective de bonnes pratiques. Il sera examiné en outre s'il est possible de développer une méthode statistique standardisée, et sous quelle forme. La mise en place d'une procédure standardisée constituerait un outil supplémen-	Reprise des essais : premier échange Examen d'une méthode standardisée : jusqu'en 2022	Cantons	Confédération : aucun Cantons : bas

Nr.	Mesure	Description	Calendrier mise en œuvre	Responsabilité	Appréciation des coûts[24] *Bas (<50'000 CHF) Moyen (50'000 - 500'000 CHF) Elevé (500'000 - 1 Mio. CHF) Très élevé (> 1 Mio. CHF)*
		taire permettant d'obtenir des indices de dysfonctionnements ou manipulations possibles. La méthode devra être applicable à la situation spécifique de chaque canton. Il conviendra également de vérifier quelles informations pourront être publiées en ce qui concerne les contrôles de plausibilité des cantons..			
B.9	Adaptations de la procédure d'autorisation	La mise en œuvre de plusieurs mesures en vue de la reprise des essais rend nécessaire d'adapter les processus inhérents à la procédure d'autorisation. Il s'agit en particulier des mesures visant à revoir les compétences en matière d'audits indépendants (mesure B.1) et de la précision des exigences relatives à la transparence (mesures C.2 et C.3). Il conviendra en outre de tenir compte aussi bien du recours à des experts indépendants dans le cadre de la procédure d'autorisation que de la gestion en continu des risques. Les catalogues des exigences de la ChF seront adaptés. La ChF examine également dans quelle mesure la décision d'autorisation générale du Conseil fédéral peut être divisée en une partie liée au système et une partie spécifique au canton.	Reprise des essais	ChF avec la participation des cantons	Confédération : aucun Cantons : aucun
B.10	Examen à long terme des processus, rôles et des tâches	Les responsabilités, les rôles et les tâches de la Confédération, des cantons et des fournisseurs de systèmes influent directement sur la conception des systèmes de vote électronique considérée sous l'angle de la sécurité. Ils seront examinés et définis dans une stratégie à long terme. La Confédération et les cantons peuvent élaborer des mesures qui tiennent compte de l'évolution de la situation en ce qui concerne le nombre de fournisseurs de systèmes, la gouvernance et les besoins de financement du vote électronique.	Long terme	GT Avenir VE	Confédération : aucun Cantons : aucun
C.	**Renforcement de la transparence et de la confiance**				
C.1	Limitation de l'électorat admissible pour les systèmes complètement vérifiables	Durant la phase d'essai, l'électorat autorisé à voter par voie électronique sera limité lors de l'utilisation de systèmes complètement vérifiables. Les plafonds seront de 30 % pour l'électorat cantonal et de 10 % pour l'électorat national. Les électeurs suisses de l'étranger continueront de ne pas être comptabilisés dans le calcul des plafonds. Le relèvement ou le cas échéant l'abrogation des plafonds sera examiné quand les systèmes complètement vérifiables auront fait leurs preuves au cours d'une phase d'essai stable.	Reprise des essais	ChF	Confédération : aucun Cantons : individuellement, en fonction du type de contrôle de l'électorat (par exemple, l'introduction d'une procédure d'enregistrement peut entraîner des coûts moyens)

Nr.	Mesure	Description	Calendrier mise en œuvre	Responsabilité	Appréciation des coûts[24] *Bas (<50'000 CHF)* *Moyen (50'000 - 500'000 CHF)* *Elevé (500'000 - 1 Mio. CHF)* *Très élevé (> 1 Mio. CHF)*
C.2	Précision des exigences concernant la publication du code source	Les exigences actuelles relatives à la publication du code source seront précisées. Exigences concernant la documentation : - Le code source et la documentation du logiciel ainsi que les fichiers contenant les paramètres d'entrée pertinents doivent être publiés. - Les guides et autres documentations complémentaires doivent être publiés afin que des personnes spécialisées puissent efficacement compiler, faire fonctionner et analyser le système dans leur propre infrastructure. - La documentation concernant l'infrastructure, les logiciels tiers et les processus d'exploitation doit être publiée dans toute la mesure du possible. - La présentation des documents publiés est conforme à la pratique courante. Exigences concernant les conditions d'utilisation : - L'accès au code source est gratuit et anonyme. - Le code source peut être utilisé à des fins idéales et notamment scientifiques. Cela inclut l'échange durant la recherche d'erreur et le droit de publication. Ce droit est accordé explicitement par le propriétaire. - Quiconque respecte les conditions d'utilisation ne sera pas poursuivi en justice. Une violation des conditions d'utilisation ne sera poursuivie que si le code source ou des parties de celui-ci sont utilisés à des fins commerciales ou productives. Les conditions d'utilisation font référence à cette limitation de responsabilité. - Il suffit de faire référence dans les termes de la licence aux conditions d'utilisation. Il convient si possible de renoncer aux déclarations d'intention de l'utilisateur. Le CoPil VE est favorable à la publication des futurs systèmes et composants de systèmes sous une licence *open source*. En outre, la Poste, en tant que fournisseur actuel du système, examine si le code source des composants de son système complètement vérifiable déjà développés peuvent également être placés sous une licence *open source*.	Reprise des essais	Exigences : ChF Publication : Cantons, fournisseur	Confédération : aucun Cantons : aucun
C.3	Gestion d'un programme de bug bounty	Un programme de bug bounty sera mis en place portant sur le code source et de la documentation publiés relatifs aux systèmes de vote électronique. Ce programme devra répondre, entre autres, aux exigences suivantes :	Reprise des essais	Exigences : ChF Mise en œuvre : Cantons, fournisseur	Confédération : participation à évaluer Cantons : élevé

Nr.	Mesure	Description	Calendrier mise en œuvre	Responsabilité	Appréciation des coûts[24] *Bas (<50'000 CHF) Moyen (50'000 - 500'000 CHF) Elevé (500'000 - 1 Mio. CHF) Très élevé (> 1 Mio. CHF)*
		- Le programme de bug bounty fonctionne en principe sans interruption. - Le signalement d'un défaut donne droit au versement d'une indemnité financière en rapport avec la gravité du défaut constaté. Le barème des indemnités doit se baser sur le barème utilisé lors du test public d'intrusion réalisé en 2019. - Le programme de bug bounty comprend trois domaines : • La recherche d'erreurs dans le code source et la documentation publiés (test statique) • La recherche d'erreurs par l'analyse du système opérationnel dans sa propre infrastructure (test dynamique) • Attaques contre l'infrastructure du fournisseur (test Internet). Le programme de bug bounty doit permettre les attaques contre l'infrastructure du fournisseur. Les attaques par DDOS et par social engineering peuvent être exclues. Les attaques contre l'infrastructure peuvent être interdites dans des cas justifiés (par exemple, lors d'une élection) - Responsabilités et traitement des signalements : • Le fournisseur de système est responsable du programme. Il permet la conduite, réceptionne les signalements et les classe par catégorie. Il communique ses décisions vis-à-vis des participants en les motivant et publie toutes les signalements de défaut qui sont confirmés. • La ChF fixe les conditions générales fondamentales. • La Confédération et les cantons ont un accès illimité aux signalements ainsi qu'aux réponses du fournisseur du système. Dans le cadre de la procédure d'autorisation, une synthèse des signalements et des mesures prises sur la base des signalements doit être fournie. - Conditions d'utilisation : Une participation anonyme et des publications concernant les défauts sont autorisées, « responsible disclosure ». La divulgation de l'identité ne peut être demandée que pour le paiement d'une indemnité dans le cadre du programme de bug bounty. La ChF détermine les exigences en consultation avec les cantons et examine l'éventualité d'une participation financière. Une possibilité de processus de réclamation pour les participants qui ne seraient pas			Mise en œuvre avec test Internet périodique (compensation non comprise) : – Unique : 230'000-290'000 CHF – Récurrent : 55'000-70'000 CHF / an Mise en œuvre avec test Internet continu (compensation non comprise) : – Unique : 255'000-360'000 CHF – Récurrent : 550'000-650'000 CHF / an

Nr.	Mesure	Description	Calendrier mise en œuvre	Responsabilité	Appréciation des coûts[24] *Bas (<50'000 CHF)* *Moyen (50'000 - 500'000 CHF)* *Elevé (500'000 - 1 Mio. CHF)* *Très élevé (> 1 Mio. CHF)*
		d'accord avec la décision du fournisseur de système doit être également examinée. Pour la reprise des essais, le test Internet doit être effectué sur le système productif. Ensuite, une décision sur la suite de la procédure peut être prise sur la base de l'expérience acquise. Il existe deux options : le test Internet peut être effectué de manière répétée sur le système productif ou comme un test continu sur un système jumeau.			
C.4	Publication des rapports d'audit pertinents pour l'autorisation	La Confédération, les cantons et le fournisseur de système œuvrent à la transparence à l'égard du public en ce qui concerne les résultats des audits en lien avec la procédure d'autorisation. Les rapports, justificatifs et certificats qui doivent être fournis au sens du chiffre 5 de l'annexe de l'OVotE doivent être publiés. Les rapports d'audit publiés doivent être compréhensibles. S'il y est fait référence à d'autres documents, ces derniers doivent également être publiés en règle générale. Il peut être renoncé à la publication dans des cas justifiés (par exemple, si la publication fait augmenter un risque, ou si des raisons de protection des données ou des directives de sécurité internes s'opposent à la publication). Les réponses que l'organisme contrôlé prépare en relation avec les rapports d'audit publiés doivent également être publiées.	Reprise des essais	ChF, cantons, fournisseur	Confédération : éventuellement bas Cantons : aucun
C.5	Lors des scrutins fédéraux, publication du résultat des votes exprimés à travers le vote électronique	Il s'agit d'établir la transparence à l'égard du public à propos des résultats des votes exprimés par voie électronique. Les cantons publieront donc les résultats des élections et des votations fédérales pour le canal de vote électronique. Cela doit permettre à la population de comparer les résultats du vote électronique avec le résultat global et d'exécuter un contrôle de plausibilité. Des exceptions doivent être prévues afin de garantir le secret du vote.	Reprise des essais	Exigences : ChF Publication : Cantons	Confédération : aucun Cantons : bas
C.6	Une participation accrue du public	La confédération et les cantons élaborent un concept avec la participation du fournisseur de système visant à renforcer la participation du public. Outre la classe politique, les experts et les groupes d'intérêt, l'accent doit également être mis sur le grand public. Ce concept doit inclure des plans de communication active. La mise en œuvre de certaines activités doit être évaluée en vue de la reprise des essais.	Concept : reprise des essais	ChF avec la participation des cantons et fournisseur	<u>Concept</u> Confédération : bas Cantons : aucun <u>Mise en œuvre</u> Selon les activités ; 2021 coûts bas pour la Confédération

Nr.	Mesure	Description	Calendrier mise en œuvre	Responsabilité	Appréciation des coûts[24] *Bas (<50'000 CHF)* *Moyen (50'000 - 500'000 CHF)* *Elevé (500'000 - 1 Mio. CHF)* *Très élevé (> 1 Mio. CHF)*
D.	**Renforcement des liens avec les milieux scientifiques**				
D.1	Elaboration d'un concept pour le soutien scientifique des essais et le dialogue avec des experts externes	Les essais de vote électronique devront faire l'objet d'une étude et d'un suivi scientifiques permanents. En outre, la Confédération et les cantons entretiendront un dialogue permanent avec la communauté scientifique et les services spécialisés compétents. Ils poseront des questions, répondront à des suggestions, participeront activement aux discussions et fourniront l'infrastructure et les ressources nécessaires aux échanges. La Confédération et les cantons commanderont par ailleurs des études scientifiques sur des sujets exigeant des recherches plus approfondies. La Confédération et les cantons élaboreront en collaboration avec les représentants de la communauté scientifique un concept pour le suivi scientifique et le dialogue avec des experts externes pour la période 2022-2025, ainsi que pour le financement. Le développement de ce concept sera placé sous la responsabilité de la ChF.	Concept : 2021	ChF avec la participation des cantons	Confédération : bas Cantons : bas
D.2	Participation d'experts indépendants	La Confédération et les cantons devraient associer à leurs travaux des experts ou services spécialisés indépendants actifs dans les disciplines scientifiques concernées, ainsi que d'autres organisations si cela devait se révéler utile et apporter une plus-value, en particulier pour les mesures définies dans le cadre de la restructuration.	Dans le cadre des mesures individuelles	ChF avec la participation des cantons	Estimation dans le cadre des mesures individuelles
D.3	Elaboration d'un concept pour la mise en place d'un comité scientifique	Un comité scientifique sera mis en place pour conseiller la Confédération et les cantons. Ce comité devrait assumer des tâches de conseil dans la perspective d'une collaboration avec la communauté scientifique (au sens des mesures D.1 et D.2) et devrait également être en mesure d'accomplir lui-même certaines tâches. A cette fin, la Confédération et les cantons élaborent un concept pour les années 2022-2025.	Concept : 2022	ChF avec la participation des cantons	<u>Elaboration du concept</u> Confédération : aucun Cantons : aucun