Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF
Section des droits politiques

1er mars 2023

Processus de gestion des risques Vote électronique de la Chancellerie fédérale

Table des matières

1 Introduction

1.1 Contexte

L'ampleur des risques ne dépend pas uniquement du respect des exigences définies dans l'ordonnance de la Chancellerie fédérale (ChF) sur le vote électronique (OVotE ; RS 161.116). Elle dépend également des menaces telles qu'elles se présentent à un moment donné. De même, une accumulation d'incidents liés à la sécurité lors de l'exploitation des systèmes ou de nouvelles connaissances sur la situation générale des menaces peuvent entraîner une modification de l'évaluation des risques. Ces réflexions ont été intégrées dans l'OVotE : Les cantons doivent évaluer en permanence les risques liés au vote électronique (cf. art. 4 OVotE). Si, malgré les mesures prises, les risques ne sont pas suffisamment faibles, des mesures supplémentaires doivent être prises afin de les réduire (cf. art. 9 OVotE). Les cantons doivent remettre à la ChF leur évaluation actualisée des risques avant chaque scrutin pour lequel le canal de vote électronique sera utilisé (cf. art. 15, al. 1 let. a, OVotE). La ChF vérifie la plausibilité de l'évaluation en se référant aux mesures mises en œuvre et s'assure que le niveau des risques considérés est suffisamment faible. Sur la base de ces documents, la ChF décide si elle autorise la réalisation d'un essai de vote électronique.

Ainsi, le fait que les conditions d'octroi de l'agrément pour les essais de vote électronique soient effectivement remplies ne dépend pas exclusivement du respect des exigences techniques et organisationnelles. C'est avant tout l'objectif général qui prime, à savoir que les objectifs de sécurité tels que définis dans la base légale (cf. art. 4 al. 3 OVotE) soient protégés autant que possible et que les risques qui les menacent soient connus, évalués et mitigés par des mesures appropriées afin qu'ils demeurent à un niveau suffisamment faible. Une gestion responsable des risques passe naturellement par une gestion efficace des risques tant au niveau fédéral que cantonal.

1.2 Objectifs

Avec la gestion des risques Vote électronique, la ChF poursuit les objectifs suivants :

- une culture de gestion responsable des risques liés au vote électronique est mise en place tant au niveau de la direction qu'au niveau opérationnel,
- les risques en lien avec le vote électronique demeurent à un niveau acceptable selon les critères d'évaluation définis,
- la ChF et les cantons connaissent les risques liés au vote électronique. Les responsables au niveau de la direction et au niveau opérationnel ont connaissance des informations qui les concernent, et
- la ChF et les cantons réagissent de manière efficace et cohérente aux événements affectant les risques.

1.3 Champ d'application

Le présent document ne s'applique qu'à la gestion des risques dans le cadre du projet Vote électronique de la ChF. Les cantons et leurs fournisseurs de services en lien avec le vote électronique disposent de leur propre processus de gestion des risques. Pour ce qui est de sa gestion des risques, la ChF met en œuvre son propre processus de gestion des risques établi sur le modèle de la Confédération[1]. Les risques présentés dans ce document y sont intégrés sous une forme agrégée.

1.4 Cycle de vie

Le présent document est établi et maintenu par la ChF. Elle peut, pour ce faire, s'appuyer sur les compétences d'experts de la Confédération ou issus des milieux scientifiques ou de l'industrie.

Le présent document doit être revu sur une base annuelle et selon l'état des connaissances.

---

[1] www.efv.admin.ch > Thèmes > Politique budgétaire, Bases > Politique de gestion des risques et de l'assurance

2 Responsabilités dans le cadre de la tenue de scrutin fédéraux

2.1 Des cantons

L'organisation des élections et des votations fédérales relève de la compétence des cantons. Par conséquent, les cantons sont responsables de la bonne exécution des élections et des votations dans le domaine du vote électronique également (cf. art. 14 OVotE). Dans ce cadre, ils élaborent une appréciation des risques relative aux essais de vote électronique en application de l'art. 4 de l'OVotE. Cette appréciation, le cas échéant accompagnée de celles des éventuels fournisseurs des cantons, sert à démontrer que les risques sont à un niveau suffisamment faible et que les cantons en gardent la maitrise.

2.2 De la Chancellerie fédérale

La ChF est responsable des points suivants dans le domaine du vote électronique :

- **De manière générale :**
  - La ChF veille à ce que les droits populaires puissent être exercés dans le cadre de la Constitution fédérale et de la législation sur les droits politiques et à ce que toutes les votations et élections fédérales se déroulent correctement (art. 1, al. 4, let. a, Ordonnance sur l'organisation de la ChF, Org ChF, RS 172.210.10).
  - Préparation et exécution de la loi fédérale sur les droits politiques (LDP ; RS 161.1) et de l'ordonnance sur les droits politiques (ODP ; RS 161.11)
  - Définition et exécution des exigences d'agrément pour l'utilisation du canal de vote électronique dans l'ordonnance de la ChF (OVotE)
  - Observation des développements politiques, techniques et juridiques dans le domaine du vote électronique et anticipation des mesures correspondantes (en particulier pour garantir la sécurité des systèmes et un contrôle et une surveillance efficaces, pour renforcer la transparence et la confiance ainsi que les liens avec les milieux scientifiques)
  - Implication du public et des milieux spécialisés (art. 27*l* ODP)
  - Information du public sur le vote électronique en général, sur les exigences légales de la Confédération, sur l'état du projet Vote électronique et sur les développements d'importance nationale et internationale
  - La ChF veille à un suivi scientifique des essais de vote électronique (art. 27*o*, al. 2 et 3 ODP)

- **Direction opérationnelle et technique du projet Vote électronique :**
  - Coordination des projets cantonaux
  - Administration des organes du projet Vote électronique
  - Définition de mesures et mise en œuvre des mesures décidées relevant de la responsabilité de la ChF
  - Collaboration avec les services internes de la Confédération et recours à des experts indépendants dans l'accomplissement des tâches de la ChF (art. 27*o*, al. 1 ODP)
  - Intégration et mise en œuvre du projet dans le cadre de la stratégie suisse de cyberadministration, collaboration en la matière avec l'administration numérique suisse, attribution et suivi de projets cofinancés

- **Autorisation et agrément d'essais de vote électronique :**
  - Vérification du respect des exigences fédérales pour l'octroi des autorisations générales et des agréments (y compris la conduite d'un contrôle indépendant des systèmes et de leur exploitation, la publication des rapports d'audit et l'appréciation des risques au niveau national)
  - Approbation ou rejet des demandes d'agrément

– Traitement des demandes des cantons et recommandation au Conseil fédéral d'approuver ou de rejeter les demandes d'autorisation générale

Elle élabore dans ce cadre une appréciation des risques qui se basent sur les processus et activités qui sous-tendent ces missions (cf. ch. 4.1).

3 Processus de gestion des risques

Les risques sont identifiés, évalués et traités selon les conditions définies dans les chapitres suivants, en grande partie repris de la méthodologie OCTAVE Allegro. Cette méthodologie est également à la base du Guide de la ChF pour l'appréciation des risques vote électronique[2]. En utilisant une base commune, il est possible de garantir un meilleur alignement et une meilleure compréhension des risques par les différents acteurs.

Les risques identifiés, évalués et traités sont ensuite repris dans le processus de gestion des risques de la Confédération sous une forme agrégée.

3.1 Identification

L'identification des risques passe tout d'abord par l'identification des processus clés de la ChF en matière de vote électronique et des éléments nécessaires à la bonne exécution de ces processus. Ces éléments sont nommés actifs dans la suite de ce document. Pour chacun de ces actifs, s'ensuit une analyse des menaces qui pourraient le compromettre et ainsi nuire à la réalisation des objectifs de sécurité. Les menaces identifiées dont l'impact sur les objectifs de sécurité est significatif sont ensuite regroupées dans une liste de risques.

3.2 Analyse et évaluation

Pour chaque risque, les conséquences de sa réalisation doivent être analysées. Ces conséquences sont considérées en l'absence de toute mesure de mitigation. Elles représentent le pire scénario auquel pourrait conduire le risque et sont représentées sous une forme narrative. Elles doivent ensuite faire l'objet d'une évaluation selon les critères de mesure du risque. Ces critères sont un ensemble de mesures qualitatives qui permettent d'évaluer les effets d'un risque sur la mission de la ChF. Ils doivent être consistants et refléter la perspective de la ChF afin de permettre de prendre des décisions cohérentes pour la mitigation des risques. En outre, ils sont pondérés selon leur importance pour l'accomplissement de la mission de la ChF.

Les critères de mesure du risque de la ChF en matière de vote électronique sont présentés dans la table qui suit. Si plusieurs lignes sont définies pour un domaine, la condition impliquant la plus grande sévérité prévaut.

Domaines d'impact	**Critères de mesure du risque**			
	Bas (1)	**Moyen (2)**	**Haut (3)**	**Poids**
Réputation et confiance	La crédibilité des autorités fédérales n'est pas ou que légèrement menacée.	La crédibilité des autorités fédérales est moyennement menacée.	La crédibilité des autorités fédérales est fortement menacée.	5
	La validité des résultats du scrutin n'est pas mise en doute.	La validité des résultats du scrutin est peu mise en doute.	La validité des résultats du scrutin est largement mise en doute.	

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

Domaines d'impact	Critères de mesure du risque			
	Bas (1)	**Moyen (2)**	**Haut (3)**	**Poids**
Légal	Le résultat du scrutin peut être validé sans délais par le Conseil fédéral.	Le résultat du scrutin peut être validé par le Conseil fédéral moyennant un certain délais.	Le résultat du scrutin ne peut pas être validé par le Conseil fédéral.	5
	L'intégrité du scrutin est intacte.	Une manipulation isolée des votes a eu lieu.	Une manipulation systématique des votes a eu lieu.	
	Le secret du vote n'a pas fait l'objet de violation.	Le secret du vote a été violé de manière isolée.	Le secret du vote a été systématiquement violé.	
Viabilité du canal de vote électronique	La poursuite du vote électronique n'est pas ou que légèrement remise en question.	La poursuite du vote électronique est sérieusement remise en question.	Le vote électronique sera très probablement interrompu.	3
Finance	Les coûts récurrents du projet vote électronique de la ChF n'augmentent pas.	Les coûts récurrents du projet vote électronique de la ChF augmentent de manière modérée.	Les coûts récurrents du projet vote électronique de la ChF augmentent significativement.	3
	Il n'y a pas d'augmentation ponctuelle des coûts ou elle reste modérée.	Il y a une augmentation ponctuelle des coûts significative.		
Ressources	La charge de travail n'augmente pas ou seulement de manière ponctuelle et modérée.	La charge de travail augmente de manière durable mais modérée ou de manière ponctuelle mais significative.	La charge de travail augmente de manière durable et significative.	1

La probabilité d'occurrence des risques est ensuite évaluée selon une échelle qui se base sur une période de 3 ans, soit approximativement 10 scrutins, et qui est établie sur la base d'estimations subjectives. Cette échelle sera adaptée au besoin en fonction des connaissances acquises.

- Haut (3) : Scénario hautement probable : il est fort probable qu'un incident se produise au cours des dix prochains scrutins (probabilité supérieure à 30 %).
- Moyen (2) : Scénario possible : la probabilité qu'un incident se produise au cours des dix prochains scrutins est normalement nulle, mais il faut anticiper un éventuel incident (probabilité de l'ordre de 3 à 30 %).
- Bas (1) : Scénario improbable : aucun incident ne se produit au cours des dix prochains scrutins (probabilité inférieure à 3 %).

Cette probabilité s'applique uniquement au risque, à savoir à l'événement caractérisant le risque. Elle ne s'applique pas au scénario décrivant les conséquences de la réalisation du risque.

3.3 Traitement

La ChF décide du traitement du risque en fonction de son score et de sa probabilité d'occurrence.

Elle peut :

Probabilité	Score		
	32 – 49	22 – 31	17 – 21
Haut	Mitiger	Mitiger	Mitiger Surveiller
Moyen	Mitiger	Mitiger Surveiller	Mitiger Surveiller Accepter
Bas	Mitiger Surveiller	Mitiger Surveiller Accepter	Mitiger Surveiller Accepter

3.4 Risques résiduels

A l'issue de l'étape de traitement des risques, les risques résiduels doivent être identifiés et évalués. Ils doivent ensuite faire l'objet d'une acceptation explicite par la ChF pour le que vote électronique puisse être mis en œuvre.

3.5 Suivi et revue des risques

L'ensemble des risques doit être revu par la ChF au moins annuellement. Cette revue doit considérer les événements intervenus depuis la dernière revue qu'ils soient de nature politique (p. ex. interventions parlementaires, nouvelles réglementations), sécuritaire (p. ex. failles de sécurité affectant le système ou des éléments de son infrastructure) ou technique (p. ex. développement de nouvelle technologie améliorant ou péjorant la sécurité du vote électronique).

En sus de la revue annuelle, une identification, une évaluation et un éventuel traitement des risques spécifiques à chaque scrutin doivent être menés. Ces activités doivent prendre en considération les événements intervenus depuis la dernière revue ainsi que les aspects particuliers liés au scrutin.

3.6 Documentation

Le résultat de l'ensemble des étapes du processus de gestion des risques doit être documenté dans l'appréciation des risques Vote électronique de la ChF. Ce document doit être revu par une entité compétente et validé par la ChF. Il est ensuite publié sur le site Internet de la ChF et est transmis aux cantons concernés par les essais de vote électronique.

3.7 Intégration des risques vote électronique dans la gestion des risques de la ChF et de la Confédération

Pour la gestion de ses risques, la ChF suit son propre processus de gestion des risques établi sur le modèle de celui de la Confédération. Les risques y sont systématiquement identifiés, documentés et évalués. Les risques présentés dans ce document sont repris sous une forme agrégée à un niveau pertinent pour la ChF. Ils sont revus dans ce cadre par le gestionnaire des risques de la ChF.

4 Éléments fondamentaux pour l'appréciation des risques Vote électronique de la ChF

4.1 Processus / activités clés

Les responsabilités de la ChF dans le cadre du vote électronique (cf. ch. 2.2) sont couvertes par les processus et activités suivants :

1. [Bases légales] Établir et maintenir la base légale des essais de vote électronique
   - Maintenir une veille technologique, sociologique et légale dans le domaine du vote électronique
   - Maintenir une veille en matière de sécurité de l'information

- Réviser les ordonnances ODP et OVotE

2. [Agrément] Agréer l'utilisation d'un système de vote électronique pour un canton
   - Garantir le contrôle indépendant du système et/ou du canton
   - Contrôler les non-conformités
   - Vérifier les conditions d'agrément
   - Décider de l'octroi ou non de l'agrément
   - Préparer la décision du Conseil fédéral relative à l'octroi ou non de l'autorisation générale
3. [Surveillance] Surveiller la bonne conduite de la phase d'essai, y inclus des scrutins
   - Définir, collecter et mettre à disposition du public les chiffres clés des essais de vote électronique (p. ex. participation par le canal de vote électronique, nombre de bulletins par objet, candidat ou liste)
   - Surveiller et accompagner le bon traitement des signalements d'irrégularité ou de défaut pendant les scrutins au niveau fédéral
   - Accompagner et soutenir les projets cantonaux
4. [Communication] Établir et mettre en œuvre une stratégie de communication factuelle et transparente
5. [Accompagnement] Mettre en place un accompagnement scientifique des essais de vote électronique
   - Établir un dialogue avec les milieux scientifiques
   - Étudier les essais pour identifier les améliorations possibles (p. ex. accessibilité, confiance et acceptation des électeurs, renforcement de la vérifiabilité)
   - Analyser, planifier et mettre en œuvre les améliorations identifiées
6. [Risques] Gérer les risques de la ChF relatifs au vote électronique
   - Établir et maintenir un guide pour l'appréciation des risques
   - Établir et maintenir une appréciation des risques
   - Maintenir une veille en matière de menaces
7. [Crises] Gérer les crises relatives au vote électronique qui prennent une ampleur nationale
   - Établir et maintenir une convention de crise commune
   - Établir et maintenir des scénarios de crise
   - Organiser et conduire des exercices de crise

4.2 Catalogue des actifs

Dans le contexte de l'appréciation des risques, les actifs sont entendus comme l'ensemble des éléments tangibles et intangibles qui sont nécessaires à la ChF pour exécuter les processus et activités clés définis dans le chapitre précédent. Le tableau suivant en présente la liste avec une référence aux processus qui dépendent d'eux et les raisons de leur inclusion dans l'appréciation des risques.

Actifs	**Processus dépendant**	**Pourquoi cet actif est important**	**Conséquences de son altération**	**Exigence de sécurité**
Résultats du scrutin fédéral	Surveillance Communication	Les résultats du scrutin doivent être conformes à la volonté des votants et disponibles.	Une perte de confiance dans le système politique et le canal de vote électronique.	Intégrité Disponibilité
Confiance des électeurs	Bases légales Communication	Sans confiance dans le canal de vote électronique, ce dernier ne peut être utilisé.	Possible fin du vote électronique.	Disponibilité

Actifs	Processus dépendant	Pourquoi cet actif est important	Conséquences de son altération	Exigence de sécurité
ODP et OVotE	Bases légales Agrément	La base légale est nécessaire à la conduite des essais et elle en fixe les conditions de sécurité.	Si les bases légales préconisent un niveau de sécurité trop bas, un système avec un niveau de sécurité inadéquat pourrait être agrée.	Intégrité
Experts indépendants et compétents	Bases légales Agrément Communication Accompagnement Risques Crises	Les experts indépendants sont nécessaires au contrôle des systèmes, à l'amélioration des technologies disponibles et préconisées, à la surveillance des essais ainsi qu'au débat public.	En cas de manque d'experts compétents, la procédure d'agrément pourrait être ralentie, les exigences légales pourraient ne plus être adéquates et un débat factuel et objectif ne pourrait avoir lieu.	Disponibilité
Cantons participants aux essais	Bases légales Agrément Surveillance Communication Risques Crises	Les cantons qui conduisent des essais de vote électronique collectent une expérience et des informations nécessaires afin de tirer des conclusions des essais et d'améliorer le canal de vote électronique. Ils ont en outre un rôle très important dans l'établissement de la confiance des électeurs et la promotion de la participation du public.	Si aucun canton ne souhaite conduire d'essai, le vote électronique ne pourra pas progresser.	Disponibilité
Fournisseurs de système	Agrément Surveillance Communication Risques Crises	La disponibilité d'un fournisseur fiable et les mesures qu'il met en place pour la protection du système sont cruciaux pour la confiance des électeurs.	S'il n'existe aucun fournisseur de système capable de remplir les exigences de la ChF, aucun essai ne pourra être conduit et le vote électronique ne pourra pas progresser. En outre, un fournisseur peu convainquant peut avoir une influence négative sur la confiance des électeurs.	Disponibilité

Actifs	Processus dépendant	Pourquoi cet actif est important	Conséquences de son altération	Exigence de sécurité
Scrutin fiable avec vote électronique	Agrément Surveillance Communication Risques Crises	Les résultats du scrutin doivent être conformes à la volonté des votants et disponibles. La ChF garanti un contrôle efficace des essais menés en conformité avec les exigences fédérales. Pour ce faire elle a besoin que les scrutins avec vote électronique soient conduits et contrôlés de manière adéquate.	Si le scrutin est compromis, il pourrait en résulter une perte de confiance dans le système politique et les autorités. Des recours contre les résultats du scrutin pourraient intervenir et conduire à la répétition du scrutin.	Intégrité Confidentialité Disponibilité

4.3 Catalogue des risques

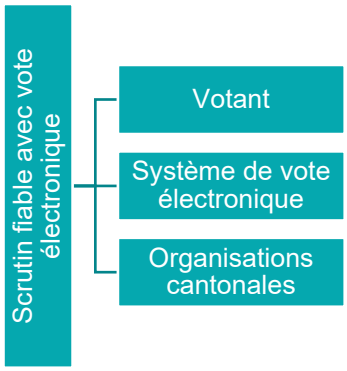
Le catalogue des risques identifiés sur la base des actifs présentés dans le chapitre précédant figure dans le document d'appréciation des risques Vote électronique de la ChF.

5 Exemple de mise en œuvre du processus de gestion des risques

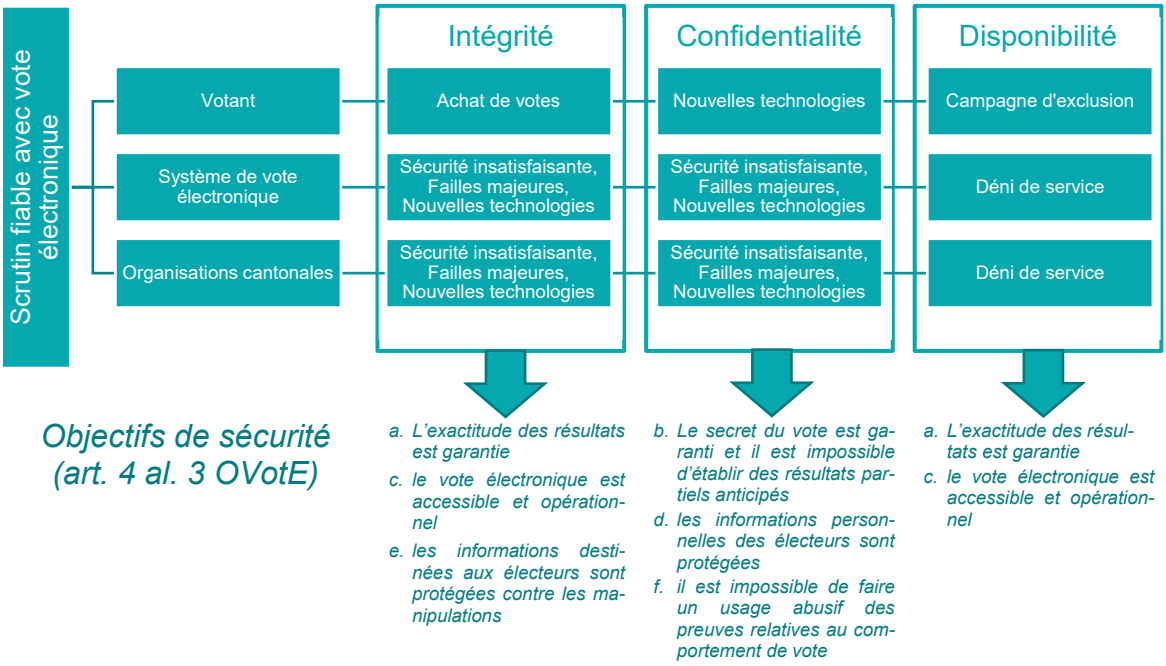
Ce chapitre vise à illustrer la démarche présentée dans ce document. Il n'a pas vocation à représenter un cas réel de manière exhaustive.

5.1 Identification

En suivant la méthode décrite dans ce document, on part d'abord d'un actif et on détermine les éléments qui peuvent avoir une influence sur cet actif et les exigences de sécurité (intégrité, confidentialité, disponibilité) qui lui permettent de contribuer aux objectifs de sécurité (cf. art. 4 al. 3 OVotE). Pour l'actif Scrutin fiable avec vote électronique, cela donne :



Il s'agit ensuite de déterminer ce qui pourrait nuire à chacune des exigences de sécurité applicables à l'actif au regard des éléments identifiés au préalable. On obtient ainsi un ensemble de menaces :



Ces menaces peuvent maintenant être décrites sous la forme de risques qui présentent un scénario possible de réalisation de la menace. Il leur est également attribué un identifiant unique qui permet de les référencer tout au long de l'appréciation. Afin de garder cet exemple concis, seul un risque sera présenté ici :

Identifiant	Description	Actifs
Risque_1	La Confédération a autorisé l'utilisation d'un système dont les mesures de sécurité ne satisfont pas les exigences légales.	Scrutin fiable avec vote électronique
Objectifs de sécurité (art. 4 al.3 OVotE)		
a. l'exactitude des résultats est garantie b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés c. le vote électronique est accessible et opérationnel d. les informations personnelles des électeurs sont protégées e. les informations destinées aux électeurs sont protégées contre les manipulations f. il est impossible de faire un usage abusif des preuves relatives au comportement de vote		

5.2 Analyse et évaluation

En se basant sur la menace identifiée et documentée dans le risque, il s'agit maintenant d'évaluer la probabilité qu'elle se concrétise. Pour ce faire, il faut reprendre l'échelle d'évaluation définie dans le chapitre 3.2. Cette estimation s'entend avant la mise en œuvre de toute mesure. En l'occurrence, la probabilité est estimée à Moyenne car s'il est très peu probable que la Confédération autorise un système qui ne satisfait pas les exigences légales, il faut toutefois l'anticiper.

Risque_1	***Autorisation d'un système défaillant***	
Menace	La Confédération a autorisé l'utilisation d'un système dont les mesures de sécurité ne satisfont pas les exigences légales.	
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés c. le vote électronique est accessible et opérationnel d. les informations personnelles des électeurs sont protégées e. les informations destinées aux électeurs sont protégées contre les manipulations f. il est impossible de faire un usage abusif des preuves relatives au comportement de vote	
Conséquences		
Évaluation		**Initiale**
	Probabilité	Moyenne

Il faut maintenant décrire ce qu'il se passerait si la menace venait à se réaliser. On se base ici sur le pire scénario que l'on décrit de façon narrative pour former les conséquences.

Risque_1	***Autorisation d'un système défaillant***	
Menace	La Confédération a autorisé l'utilisation d'un système dont les mesures de sécurité ne satisfont pas les exigences légales.	
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés c. le vote électronique est accessible et opérationnel d. les informations personnelles des électeurs sont protégées e. les informations destinées aux électeurs sont protégées contre les manipulations f. il est impossible de faire un usage abusif des preuves relatives au comportement de vote	
Conséquences	Si un usage abusif du système ne peut être écarté et que la participation électronique peut changer le résultat du scrutin, le scrutin devra très probablement être déclaré nul. La réputation des autorités sera gravement entachée et les essais de vote électronique devront être suspendus.	
Évaluation		**Initiale**
	Probabilité	Moyenne

Il convient maintenant de transformer cette analyse qualitative (les conséquences) en analyse quantitative. Cette transformation ne peut pas se faire uniquement selon une formule mathématique. Il faut utiliser sa connaissance du terrain et du bon sens et les transposer en utilisant la table des critères de mesure du risque définie dans le chapitre 3.2 et en appliquant également la pondération qui s'y trouve. L'analyse quantitative donne un score de risque qui permet ensuite de prioriser le traitement des risques.

Domaines d'impact	Critères de mesure du risque				Score
	Bas (1)	**Moyen (2)**	**Haut (3)**	**Poids**	
Réputation et confiance	La crédibilité des autorités fédérales n'est pas ou que légèrement menacée.	La crédibilité des autorités fédérales est moyennement menacée.	La crédibilité des autorités fédérales est fortement menacée.	5	3 x 5 = 15
	La validité des résultats du scrutin n'est pas mise en doute.	La validité des résultats du srutin est peu mise en doute.	La validité des résultats du scrutin est largement mise en doute.		
Légal	Le résultat du scrutin peut être validé sans délais par le Conseil fédéral.	Le résultat du scrutin peut être validé par le Conseil fédéral moyennant un certain délais.	Le résultat du scrutin ne peut pas être validé par le Conseil fédéral.	5	3 x 5 = 15
	L'intégrité du scrutin est intacte.	Une manipulation isolée des votes a eu lieu.	Une manipulation systématique des votes a eu lieu.		
	Le secret du vote n'a pas fait l'objet de violation.	Le secret du vote a été violé de manière isolée.	Le secret du vote a été systématiquement violé.		
Viabilité du canal de vote électronique	La poursuite du vote électronique n'est pas ou que légèrement remise en question.	La poursuite du vote électronique est sérieusement remise en question.	Le vote électronique sera très probablement interrompu.	3	3 x 3 = 9
Finance	Les coûts récurrents du projet vote électronique de la ChF n'augmentent pas.	Les coûts récurrents du projet vote électronique de la ChF augmentent de manière modérée.	Les coûts récurrents du projet vote électronique de la ChF augmentent significativement.	3	2 x 3 = 6
	Il n'y a pas d'augmentation ponctuelle des coûts ou elle reste modérée.	Il y a une augmentation ponctuelle des coûts significative.			
Ressources	La charge de travail n'augmente pas ou seulement de manière ponctuelle et modérée.	La charge de travail augmente de manière durable mais modérée ou de manière ponctuelle mais significative.	La charge de travail augmente de manière durable et significative.	1	2 x 1 = 2
Score total					**47**

A l'issue de la phase d'analyse et d'évaluation, le risque est décrit comme suit :

Risque_1	***Autorisation d'un système défaillant***
Menace	La Confédération a autorisé l'utilisation d'un système dont les mesures de sécurité ne satisfont pas les exigences légales.
Objectifs de sécurité *(art. 4 al. 3 OVotE)*	a. l'exactitude des résultats est garantie b. le secret du vote est garanti et il est impossible d'établir des résultats partiels anticipés c. le vote électronique est accessible et opérationnel d. les informations personnelles des électeurs sont protégées e. les informations destinées aux électeurs sont protégées contre les manipulations f. il est impossible de faire un usage abusif des preuves relatives au comportement de vote
Conséquences	Si un usage abusif du système ne peut être écarté et que la participation électronique peut changer le résultat du scrutin, le scrutin devra très probablement être déclaré nul. La réputation des autorités sera gravement entachée et les essais de vote électronique devront être suspendus.
Évaluation	

	Initiale	
Probabilité	Moyenne	
Critères	**Valeur**	**Score**
Réputation et confiance	Haut (3)	15
Légal	Haut (3)	15
Viabilité	Haut (3)	9
Finance	Moyen (2)	6
Ressources	Moyen (2)	2
Score d'impact		**47**

5.3 Traitement

Le score et la probabilité du risque détermine les actions possibles en fonction de la stratégie de traitement des risques définie au chapitre 3.3. Nous avons ici un risque avec une probabilité Moyenne et un score de 47 :

Probabilité	**Score**		
	32 – 49	**22 – 31**	**17 – 21**
Haut	Mitiger	Mitiger	Mitiger Surveiller
Moyen	Mitiger	Mitiger Surveiller	Mitiger Surveiller Accepter
Bas	Mitiger Surveiller	Mitiger Surveiller Accepter	Mitiger Surveiller Accepter

Il n'est donc pas possible de choisir une autre action qu'une mitigation du risque. Il faut maintenant définir les conditions de mitigation du risque. Elles peuvent agir pour diminuer la probabilité de concrétisation de la menace et/ou pour diminuer l'impact de cette concrétisation.

ID	Action	Mesures

Risque_1	Mitiger	- Exigences légales :
		  - Plafonds de 30% de l'électorat cantonal et 10% de l'électorat national (art. 27*f* ODP)
		  - Contrôle des systèmes et des modalités d'exploitation (art. 27*l* ODP et art. 10 OVotE)
		  - Publication du code source et de la documentation du système et de son exploitation (art. 11 et 12 OVotE)
		  - Participation du public (art. 13 OVotE)
		  - Détection et annonce d'incidents et de vulnérabilités en matière de sécurité; gestion des incidents en matière de sécurité et des améliorations (ch. 14 annexe OVotE)
		  - Développement et maintenance de systèmes d'information (ch. 24 annexe OVotE)
		  - Qualité du code source et de la documentation (ch. 25 annexe OVotE)
		- Gestion d'un catalogue de mesures commun de la Confédération et des cantons

Dans cet exemple, les mesures de plafonnement de l'électorat et de détection, d'annonce et de gestion des incidents et des vulnérabilités en particulier permettent d'agir sur les conséquences d'une telle menace et par là en diminue l'impact. Les mesures de contrôle indépendant et public quant à elles agissent principalement sur la probabilité de réalisation de la menace en la réduisant encore.

5.4 Risques résiduels

Les mesures de traitement du risque étant prises, il faut maintenant réévaluer le risque afin de vérifier s'il est réduit à un niveau acceptable. Cette réévaluation se conduit de la même manière que la première évaluation et permet de compléter le tableau initial.

Risque_1 Autorisation d'un système défaillant

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

Évaluation

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

Avec sa probabilité Basse et son score de 27, le risque est maintenant à un niveau qui lui permet d'être accepté.

Probabilité	Score		
	32 – 49	22 – 31	17 – 21
Haut	Mitiger	Mitiger	Mitiger Surveiller
Moyen	Mitiger	Mitiger Surveiller	Mitiger Surveiller Accepter
Bas	Mitiger Surveiller	Mitiger Surveiller Accepter	Mitiger Surveiller Accepter