Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Chancellerie fédérale ChF

Section des droits politiques

4 octobre 2022

Guide pour l'appréciation des risques

Système du vote électronique de La Poste Suisse

Numéro du dossier : 431.0-2/5/13/1

1 Glossaire

Actifs informationnels	Eléments d'une importance particulière dont il convient de protéger l'intégrité, la confidentialité et/ou la disponibilité. Ils peuvent être du matériel (p. ex. ordinateurs, serveurs, imprimantes), des logiciels (p. ex. Verifier), des informations (p. ex. codes de vérification), des éléments d'infrastructure (p. ex. locaux), des personnes (p. ex. membres du bureau électoral) ou des services (p. ex. portail d'administration). Cette notion est directement issue de la méthodologie OCTAVE Allegro.
Aides aux électeurs	Ensemble des informations qui permettent aux électeurs de suivre un processus de vote conforme aux hypothèses de sécurité. On peut y trouver par exemple la procédure de vérification de l'empreinte du certificat du portail de vote ou celle demandant la vérification des différents codes.
Backend	Serveur de vote qui comprend l'urne électronique et des composants de contrôles.
Bureau électoral	Personnes responsables du bon déroulement du scrutin selon le droit cantonal. Dans le cadre du vote électronique, les personnes qui chiffrent et déchiffrent les urnes.
Cartes à puce des administrateurs	Certificats permettant de s'authentifier sur le SDM.
Cartes à puce des membres du bureau électoral	Cartes contenant chacune une partie de la clé de chiffrement de l'urne électronique.
Carte de légitimation	Document permettant à l'électeur d'exercer son droit de vote.
Certificats de signature	Certificats permettant d'authentifier les communications entre certains éléments du système.
Certificat du portail de vote	Clé publique du portail de vote utilisée pour le chiffrement du suffrage électronique.
Code d'initialisation de la carte de légitimation	En complément des données d'identification de l'électeur, le code d'initialisation imprimé sur la carte de légitimation autorise l'électeur à saisir son vote.
Codes de contrôles du vote	Codes de vérification, code de confirmation et code de finalisation imprimés sur la carte de légitimation.
D0	Activités préparatoires du scrutin
D1	Journée de configuration des urnes, de transmission de celles-ci sur le système en ligne de La Poste Suisse et de génération des cartes de légitimation.
D2	Journée de chiffrement des urnes par le bureau électoral (y inclus la génération de la clé du bureau électoral).
D3	Journée de déchiffrement des urnes avec la clé du bureau électoral et de production des résultats du vote par internet.
D4	Journée de suppression de toutes les données conservées sur les PC, les supports de données (p. ex clés USB) et les cartes à puce concernant un scrutin. A l'issue de cette journée, les PC sont prêts pour un nouveau scrutin.
DIS (Data Integration Service)	Logiciel de La Poste Suisse installé et exploité dans l'infrastructure des cantons et permettant de générer les fichiers de la configuration du scrutin : • Données des électeurs pour la génération des cartes de légitimation par le service de génération idoine ; • Données du scrutin pour l'importation dans le portail d'administration.

Données d'identification de l'électeur	Eléments permettant d'identifier l'électeur qui ne figurent pas sur la carte de légitimation (p. ex. date ou année de naissance, identification dans un guichet virtuel).
Journaux et historiques (logs)	Ensemble des traces permettant de s'assurer du bon fonctionnement du processus de vote ; le cas échéant d'en investiguer les éventuels dysfonctionnements. Ils peuvent aussi bien avoir une forme numérique qu'être consignés sous forme papier.
Logiciel du contrôle des habitants	Logiciel permettant de générer le ou les fichiers eCH-0045 contenant la liste des électeurs.
Logiciel pré-vote	Logiciel permettant de générer les fichiers eCH-0157 et/ou eCH-0159 contenant les paramètres du scrutin et/ou les objets du scrutin (p. ex. logiciel cantonal pour l'établissement des résultats).
Mots de passe des administrateurs	Mots de passe pour le déchiffrement du certificat contenu sur la carte à puce correspondante.
Mots de passe des membres du bureau électoral	Mots de passe permettant de déchiffrer la partie de la clé stockée sur la carte correspondante.
Objets du scrutin	Questions posées aux électeurs dans le cas d'une votation, liste électorale et liste des candidats dans le cas d'une élection. Ils sont notamment contenus dans des fichiers aux formats eCH-0159, respectivement eCH-0157.
Paramètres du scrutin	Eléments de base du scrutin comme la date de ce dernier, les dates et heures de la fenêtre de vote, le type de votation et/ou d'élection, les paramètres de sécurité (p. ex. nombre de membres du bureau électoral).
Portail d'administration	Portail web d'administration du vote par internet fourni par La Poste Suisse et utilisé par les administrateurs du vote par internet des cantons.
Portail de vote	Portail web fourni par La Poste Suisse et utilisé par les votants.
Registre des électeurs VE	Registre des électeurs ayant la possibilité de voter par voie électronique. Il est notamment contenu dans un fichier au format eCH-0045.
Résultats VE	Résultats du dépouillement de l'urne électronique. Ils sont notamment contenus dans des fichiers au format eCH-0110 et eCH-0222.
SDM (Secure Data Manager)	Logiciel de la Poste Suisse installé et exécuté dans l'infrastructure du canton. Il est déployé sur plusieurs PC distincts, déconnectés de tout réseau, ainsi que sur un PC connecté aux installations de la Poste Suisse. Il permet d'effectuer les opérations suivantes : • Gestion des informations cryptographiques pour assurer l'intégrité et la sécurité du processus de vote ; • Génération des données d'identification de la carte de légitimation ; • Génération des codes de contrôle ; • Scellement des urnes avec la clé du bureau électoral ; • Déchiffrement des votes en garantissant le secret du vote.
Service de génération des cartes de légitimation	Logiciel utilisé pour la génération des cartes de légitimation aux formats PostScript et/ou PDF.
Suffrage électronique	Suffrage dont le contenu correspond à la saisie que le votant a effectuée sur le portail de vote.
Verifier	Dispositif technique utilisé par le bureau électoral pour évaluer la preuve fournie par le backend attestant que les résultats ont été établis correctement. La Poste Suisse fourni un logiciel open

	source qui est installé sur un ordinateur hors ligne dédié et exploité par le canton.
Vote par correspondance ou à l'urne	Ensemble des bulletins de vote transmis par correspondance (y inclus par dépôt direct auprès de l'administration communale) ou par dépôt dans l'urne.

2 Contexte et but du guide

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 de l'ordonnance sur les droits politiques, 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. Elle a une grande implication dans le canal de vote électronique (art. 8*a*, al. 4 de la loi sur les droits politiques, LDP). Dans ce cadre, elle édicte des exigences techniques et organisationnelles très détaillées dans l'ordonnance de la ChF du 25 mai 2022 sur le vote électronique (OVotE).

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. 4 en relation avec l'art. 9 OVotE.

Le présent document constitue un guide pour l'établissement des appréciations des risques de la Chancellerie fédérale, des cantons et de la Poste Suisse en tant que fournisseur du système. Il décrit l'approche générale à adopter à cet égard et précise les compétences respectives. Il a pour objectifs d'assurer la complétude et la pertinence des appréciations des risques, de rendre cette activité plus accessible aux acteurs et de définir les responsabilités en la matière.

Ce guide a été établi en commun par la Chancellerie fédérale, les cantons et la Poste Suisse (ci-après la Poste). Il devra être revu périodiquement et adapté au besoin. Il reprend les exigences de la base légale et les instancie au cas particulier du système de la Poste. Si un autre système devait être utilisé, un guide spécifique à ce système devra être établi.

3 Objectifs de sécurité à traiter

L'art. 4 OVotE définit les objectifs et lignes directrices de l'établissement des appréciations des risques. En particulier, il définit à son al. 3 les différents objectifs de sécurité qui doivent être pris en compte.

4 Méthodologie de l'appréciation des risques

Le présent guide a été pensé et défini sur la base de la méthodologie d'appréciation des risques OCTAVE Allegro[1]. S'il en reprend les principaux concepts, il reste suffisamment générique pour permettre l'utilisation de toute autre méthodologie d'appréciation des risques pour autant qu'elle comprenne les activités suivantes :

(1) Etablissement d'une politique de gestion des risques
(2) Identification des processus clé
(3) Identification des actifs informationnels liés aux processus clé et définition de leurs besoins de protection
(4) Identification des éléments techniques, physiques ou les personnes dont chaque actif informationnel dépend
(5) Identification des scénarios de menaces pour chaque actif informationnel

[1] https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

(6) Identifications des risques
(7) Analyse des risques
(8) Evaluation des risques
(9) Traitement des risques

4.1 Etablissement d'une politique de gestion des risques

La politique de gestion des risques est un élément fondamental de l'appréciation des risques. Elle définit le processus d'évaluation des risques, y compris sa périodicité, les critères utilisés pour cette évaluation, la méthode de mesure de l'impact du risque et les règles de traitement des risques. Elle doit faire l'objet d'une revue régulière afin d'assurer son adéquation.

4.2 Identification des processus clé

Pour chaque phase de la gestion d'un scrutin, il convient d'identifier les différents processus clés. Ceux-ci permettront ensuite d'identifier les actifs informationnels qu'il convient de protéger.

De manière générale et dans le contexte du système de la Poste, les phases se décomposent comme suit :

- Préparation
  - Préparation des fichiers pour le vote électronique (objets du scrutin et registre des électeurs) (D0)
  - Préparation du paramétrage du scrutin (D1)
  - Préparation de l'urne électronique (D1)
  - Génération des clés de chiffrement des administrateurs du vote (D1)
  - Génération des codes (ID votant, initialisation, vérification, confirmation et finalisation) (D1)
  - Génération des cartes de légitimation (D1)
  - Impression des cartes de légitimation (D1)
  - Expédition du matériel de vote (D1)

- Initialisation
  - Initialisation de l'urne (D2)
  - Génération des clés de chiffrement des membres du bureau électoral (D2)
  - Scellement de l'urne électronique (D2)
  - Vérification Pre-vote (D2)
  - Mise à disposition de l'urne dans le VoterPortal de la Poste (D2)
  - Vote de test des administrateurs du vote (inclus dépouillement) (D2)
  - Vote de contrôle du bureau électoral (D2)
  - Mise en sécurité du matériel (D2)

- Vote
  - Ouverture du canal de vote électronique
  - Contrôle des cartes de légitimation (vote électronique, par correspondance, par dépôt ou à l'urne)
  - Fermeture du canal de vote électronique

- Clôture
  - Mixing (en ligne) : séparation des suffrages non confirmés (Cleansing) et premier mélange des suffrages (D3)
  - Téléchargement de l'urne ou des urnes (D3)
  - Vérification (VerifyOnlineTally) (D3)
  - Mélange et déchiffrement des suffrages valides (hors ligne) (D3)
  - Vérification (VerifyOfflineTally) (D3)
  - Contrôle des votes de contrôle du bureau électoral (D3)
  - Intégration des résultats des différents canaux (D3)
  - Mise en sécurité du matériel (D3)

- Post-scrutin
  - Suppression des fichiers (D4)
  - Suppression/formatage sécurisé ou destruction des supports de données (D4)
  - Destruction des mots de passe conservés (D4)
  - Destruction des cartes à puce (D4)

4.3 Identification des actifs informationnels liés aux processus clé et définition de leurs besoins de protection

La réalisation des objectifs de sécurité susmentionnés implique d'identifier les actifs informationnels, tant à l'intérieur qu'à l'extérieur de l'infrastructure. Cette identification se base sur une analyse des processus clé telle que définie au chapitre précédent.

Les actifs informationnels et responsabilités y relatives suivants sont applicables :

Actifs informationnels	**Responsabilités selon la phase du scrutin**				
	Préparation	**Initialisation**	**Vote**	**Clôture**	**Post-scrutin**
Paramètres du scrutin	Canton	Canton Poste	Poste		
Registre des électeurs VE	Canton	Canton			
Objets du scrutin	Canton	Canton Poste Imprimerie	Poste		
Aides aux électeurs		Canton Imprimerie	Canton Poste		
Cartes à puce des administrateurs	Canton	Canton	Canton	Canton	Canton
Mots de passe des administrateurs	Canton	Canton	Canton	Canton	Canton
Données d'identification de l'électeur		Canton Poste	Canton Poste		
Code d'initialisation de la carte de légitimation	Canton	Canton Poste Imprimerie	Canton Poste		
Codes de contrôle du vote	Canton	Canton Poste Imprimerie	Canton Poste		
Cartes à puce des membres du bureau électoral		Canton	Canton	Canton	Canton
Mots de passe des membres du bureau électoral		Canton	Canton	Canton	Canton
Logiciel du contrôle des habitants	Canton				
Logiciel pré-vote	Canton				
DIS		Canton			
SDM		Canton		Canton	
Service de génération des cartes de légitimation		Canton			

Actifs informationnels	Responsabilités selon la phase du scrutin				
	Préparation	**Initialisation**	**Vote**	**Clôture**	**Post-scrutin**
Portail d'administration		Canton Poste		Canton Poste	Poste
Portail de vote		Poste	Poste		
Backend		Poste	Poste	Poste	Poste
Verifier		Canton		Canton	
Certificat du portail de vote	Poste	Poste	Poste	Poste	Poste
Suffrage électronique		Canton Poste	Poste Votant	Canton Poste	Canton Poste
Vote par correspondance ou à l'urne			Canton Votant	Canton	Canton
Résultats VE				Canton	Canton
Journaux et historiques	Canton	Canton Poste	Canton Poste	Canton Poste	Canton Poste
Certificats de signature	Canton	Canton Poste		Canton Poste	

Cette table ayant un caractère générique, elle peut être complétée par les cantons selon leurs besoins. Les actifs informationnels identifiés peuvent être regroupés entre eux ou, au contraire, répartis sur plusieurs entités dans l'appréciation des risques quand cela fait sens. Dans ce cas, une correspondance doit être établie entre les groupes et les actifs informationnels tels qu'ils sont présentés ici.

Pour chaque actif informationnel, un propriétaire doit être désigné et ce dernier en définira les besoins de protection en termes de confidentialité, d'intégrité et de disponibilité. Certains actifs informationnels peuvent avoir des besoins de protection qui dépendent d'autres actifs. Il convient d'en tenir compte lors de la définition des besoins de protection de ces derniers.

4.4 Identification des éléments techniques, physiques ou les personnes dont chaque actif informationnel dépend

Les actifs informationnels identifiés peuvent être traités, enregistrés ou transmis par différents moyens (appelés conteneurs dans la méthodologie OCTAVE Allegro). Ces derniers peuvent avoir une grande influence sur la satisfaction des besoins de protection des actifs informationnels. Il convient donc de les répertorier pour chacun d'entre eux.

Un premier groupe de conteneurs constitue l'environnement technique de l'actif informationnel. Il est composé d'une part des machines (ordinateurs des utilisateurs et serveurs de l'infrastructure) et logiciels au moyen desquelles l'actif informationnel est traité, enregistré ou transmis, et d'autre part des connexions (lignes, réseaux, clés USB, etc.) utilisées pour le transmettre. Une attention particulière doit être portée aux participants du système et canaux de communication fiables dans ce cadre (p. ex. composants de contrôle, dispositif technique des vérificateurs (Verifier), composant de configuration, composant d'impression). Afin d'identifier les conteneurs techniques, on peut répondre aux questions :

- Quels systèmes d'information (logiciels) utilisent ou traitent cet actif informationnel ?
- De quelle manière cet actif informationnel est-il transmis entre les systèmes d'information ?
- Sur quel matériel informatique (hardware) peut-on trouver cet actif informationnel ?

Un second groupe constitue l'environnement physique de l'actif informationnel. Il est composé des coffres-forts et autre locaux sécurisés qui servent à son stockage mais également des formes physiques qu'un actif informationnel peut prendre comme une copie papier. Afin de les identifier, on peut répondre aux questions :

- Existe-t-il des copies papier de cet actif informationnel ?
- Existe-t-il des espaces de stockage physiques où cet actif informationnel pourrait être stocké ?

Finalement, un dernier groupe constitue l'environnement de personne de l'actif informationnel. Il est composé des différentes personnes qui ont connaissance de l'actif informationnel. Cet aspect est important dans le cas des mots de passe ou de tout élément qui doit rester secret ou dont l'intégrité est cruciale. Afin de les identifier, on peut répondre à la question :

- Quelles personnes (électeur, administrateur, personnel, vérificateurs, etc.) pourraient avoir accès à cet actif informationnel et pourraient le mémoriser ou le divulguer ?

4.5 Identification des scénarios de menaces pour chaque actif informationnel

Dans un deuxième temps, il faut parcourir chacun des éléments techniques, physiques et de personnes identifiés à l'étape précédente et déterminer quels événements pourraient mettre en danger le respect des besoins de l'actif informationnel. Ces événements peuvent être le fait d'une personne, interne ou externe, qui agit intentionnellement ou par inadvertance, de même que des dysfonctionnements. Il peut être opportun de se baser sur des arbres de menace pour conduire cette analyse de manière systématique. Sur la base des informations ainsi récoltées, il est possible d'identifier des scénarios de menaces. Il ne faut toutefois tenir compte que des menaces afférentes à l'un des objectifs de sécurité mentionnés plus haut. Les scénarios de menaces décrits au ch. 13 de l'annexe de la OVotE (cf. tableau ci-après) doivent être considérées dans cet exercice, de même que les scénarios inhérents à la possibilité de voter par plusieurs canaux.

Réf.	Description	Objectifs de sécurité concernés	Actif informationnel
13.3	Un logiciel malveillant modifie le suffrage sur la plate-forme de l'utilisateur.	Exactitude des résultats	Suffrage électronique
13.4	Un attaquant externe détourne le suffrage au moyen d'un empoisonnement du cache DNS.	Exactitude des résultats	Suffrage électronique
13.5	Un attaquant externe modifie le suffrage au moyen de la technique de « l'homme du milieu », ou « MITM ».	Exactitude des résultats	Suffrage électronique
13.6	Un attaquant externe envoie au moyen d'une attaque MITM des données corrompues qui sont nécessaires pour émettre le suffrage et qui proviennent du système en ligne (par ex. un fichier Javascript).	Exactitude des résultats	Portail de vote
13.7	Un attaquant interne manipule le logiciel, qui n'enregistre alors plus les suffrages.	Exactitude des résultats	Backend
13.8	Un attaquant interne modifie, supprime ou multiplie des suffrages.	Exactitude des résultats	Suffrage électronique
13.9	Un attaquant interne ajoute des suffrages dans l'urne électronique.	Exactitude des résultats	Backend
13.10	Une organisation hostile pénètre dans le système pour fausser le résultat.	Exactitude des résultats	Backend

Réf.	Description	Objectifs de sécurité concernés	Actif informationnel
13.11	Un attaquant interne copie du matériel de vote et l'utilise.	Exactitude des résultats	Code d'initialisation de la carte de légitimation Codes de contrôle du vote
13.12	Un attaquant externe utilise des méthodes relevant de l'ingénierie sociale pour détourner l'attention du votant des mesures de sécurité (vérifiabilité individuelle).	Exactitude des résultats	Aides aux électeurs
13.13	Un attaquant externe pénètre électroniquement, physiquement ou au moyen de procédés d'ingénierie sociale dans l'infrastructure du canton et manipule les composants de configuration ou s'empare de données de sécurité.	Exactitude des résultats	Paramètres du scrutin SDM
13.14	Un attaquant externe pénètre électroniquement, physiquement ou au moyen de procédés d'ingénierie sociale dans l'infrastructure de l'imprimerie et s'empare des codes des cartes de légitimation.	Exactitude des résultats	Code d'initialisation du de la carte de légitimation Codes de contrôle du vote
13.15	Un attaquant externe pénètre électroniquement, physiquement ou au moyen de procédés d'ingénierie sociale dans l'infrastructure de La Poste et s'empare de cartes de légitimation.	Exactitude des résultats	Code d'initialisation de la carte de légitimation Codes de contrôle du vote
13.16	Une erreur se produit dans la vérifiabilité individuelle.	Exactitude des résultats	Backend
13.17	Une erreur se produit dans la vérifiabilité universelle.	Exactitude des résultats	Backend
13.18	Un dispositif technique des vérificateurs comporte une erreur.	Exactitude des résultats	Verifier
13.19	Une « porte dérobée » est introduite dans le système via une dépendance logicielle et est mise à profit par un attaquant externe pour accéder au système.	Exactitude des résultats Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés Accessibilité et capacité opérationnelle du vote électronique Protection contre les manipulations des informations destinées aux électeurs Pas d'usage abusif des preuves relatives au comportement de vote	Portail de vote Backend
13.20	Un logiciel malveillant installé sur la plate-forme utilisateur envoie le suffrage à une organisation hostile.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	Suffrage électronique

Réf.	Description	Objectifs de sécurité concernés	Actif informationnel
13.21	Le suffrage est détourné au moyen d'un empoisonnement du cache DNS.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	Suffrage électronique
13.22	Un attaquant externe lit le suffrage au moyen d'une attaque MITM.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	Suffrage électronique
13.23	Un attaquant interne utilise la clef et déchiffre des suffrages non anonymisés.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	Cartes à puce des membres du bureau électoral Mots de passe des membres du bureau électoral Suffrage électronique
13.24	Le secret du vote est violé lors de la vérification de l'exactitude du traitement et du dépouillement.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	SDM Verifier Suffrage électronique
13.25	Un attaquant interne lit des suffrages de manière anticipée sans devoir les déchiffrer.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	Backend
13.26	Une organisation hostile pénètre dans le système pour violer le secret du vote ou pour établir des résultats partiels de manière anticipée.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	Backend
13.27	Une erreur dans le processus de chiffrement rend celui-ci inopérant ou réduit son efficacité.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	Backend Suffrage électronique
13.28	Un attaquant interne manipule le logiciel et celui-ci divulgue les suffrages.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	Backend
13.29	Un logiciel malveillant installé sur l'ordinateur de l'électeur empêche ce dernier de voter.	Accessibilité et capacité opérationnelle du canal de vote	Aides aux électeurs
13.30	Une organisation hostile mène une attaque du type « déni de service » (DOS).	Accessibilité et capacité opérationnelle du canal de vote	Portail d'administration Portail de vote
13.31	Un attaquant interne configure mal le système; le dépouillement ne peut pas se faire.	Accessibilité et capacité opérationnelle du canal de vote	Résultats VE
13.32	Un attaquant interne falsifie les preuves cryptographiques de la vérifiabilité universelle.	Accessibilité et capacité opérationnelle du canal de vote	Journaux et historiques
13.33	Une défaillance technique du système fait que le système n'est pas disponible au moment du dépouillement.	Accessibilité et capacité opérationnelle du canal de vote	Portail d'administration Backend
13.34	Un dispositif technique des vérificateurs ne fonctionne pas au moment du dépouillement.	Accessibilité et capacité opérationnelle du canal de vote	Verifier

Réf.	Description	Objectifs de sécurité concernés	Actif informationnel
13.35	Une organisation hostile pénètre dans le système pour en perturber l'exploitation, pour manipuler les informations destinées aux électeurs ou pour obtenir des preuves relatives au comportement de vote des électeurs.	Accessibilité et capacité opérationnelle du canal de vote Protection contre les manipulations des informations destinées aux électeurs Pas d'usage abusif des preuves relatives au comportement de vote	Objets du scrutin Aides aux électeurs Portail de vote Backend
13.36	Un attaquant interne vole les données concernant les adresses des électeurs.	Protection des informations personnelles concernant les électeurs	Registre des électeurs VE Logiciel du contrôle des habitants DIS SDM Service de génération des cartes de légitimation
13.37	Un logiciel malveillant influence des électeurs pendant qu'ils se forgent une opinion.	Protection contre les manipulations des informations destinées aux électeurs	Objets du scrutin Aides aux électeurs
13.38	Un attaquant interne manipule le site Internet d'information ou le portail de vote et sème la confusion dans l'esprit des électeurs.	Protection contre les manipulations des informations destinées aux électeurs	Objets du scrutin Aides aux électeurs Portail de vote
13.39	Un attaquant interne prescrit à des électeurs si et comment ils doivent voter. Après le déchiffrement, il trouve dans l'infrastructure des pièces justificatives prouvant que les électeurs se sont tenus aux instructions.	Pas d'usage abusif des preuves relatives au comportement de vote	Backend
13.40	Un attaquant externe prescrit à des électeurs si et comment ils doivent voter et leur demande une pièce justificative prouvant qu'ils se sont tenus aux instructions.	Pas d'usage abusif des preuves relatives au comportement de vote	Suffrage électronique

4.6 Identifications des risques

Un risque est la possibilité de subir un préjudice ou une perte. Il fait référence à une situation dans laquelle une personne pourrait faire quelque chose d'indésirable ou un événement pourrait provoquer un résultat indésirable et ayant un impact négatif sur la tenue des objectifs de sécurité. Un risque est composé :

- d'un événement, déterminé par un acteur, un moyen (p. ex. l'exploitation d'une ou plusieurs failles) et un actif informationnel concerné
- d'une conséquence
- d'une incertitude

Dans cette activité, il s'agit de documenter les scénarios de menaces identifiés au chapitre précédent sous la forme de risques. Il faut en particulier déterminer les conséquences qu'aurait la réalisation de chaque scénario de menace. Idéalement, toutes les conséquences devraient être documentées mais il est admis de s'en tenir à la conséquence la plus grave pour chacun des risques.

Comme le canton porte la responsabilité générale de la bonne tenue du scrutin, il doit identifier tous les risques en lien avec cette dernière dans son appréciation des risques.

Le fournisseur du système est responsable de sa bonne exploitation vis-à-vis du canton. L'identification des risques faite par le fournisseur de système doit se baser sur les risques identifiés par le canton et être étendue en fonction des moyens techniques et organisationnel engagés. Il convient là aussi d'avoir une approche systématique ainsi qu'un niveau de détails pertinent selon ces moyens. Des arbres de menaces peuvent constituer un bon outil dans ce cadre.

De manière générale, si une appréciation des risques a déjà été conduite par le passé, les risques qu'elle contenait doivent être passé en revue. Les risques toujours pertinents doivent être repris et actualisés.

Exemple :

Scénario de menace	Risque	Conséquence
Un attaquant externe pénètre électroniquement, physiquement et/ou au moyen de procédés d'ingénierie sociale dans l'infrastructure de l'imprimerie et s'empare des codes des cartes de légitimation.	Un activiste dans un domaine pour lequel le résultat du scrutin peut avoir une influence se fait passer pour un réparateur d'imprimante et profite de son accès à l'infrastructure pour y installer une caméra lui permettant de voir les codes d'initialisation des cartes de légitimation.	La caméra n'est pas trouvée et l'attaquant a enregistré une grande quantité de codes d'initialisation. Il trouve sur les réseaux sociaux une partie des dates de naissance correspondantes et il les utilise pour saisir des votes. Certains électeurs étonnés de ne pouvoir utiliser leur matériel contactent la chancellerie d'état. Cette dernière suspend le canal de vote électronique et débute une enquête. Les médias sont alertés de l'affaire et en font leur gros titre, ce qui génère un gros effort de communication pour la chancellerie d'état. Des recours sont interjetés et aboutissent à l'annulation du scrutin.

4.7 Analyse des risques

L'analyse des risques est une entreprise complexe. Dans le cadre d'une évaluation structurée des risques, il convient d'analyser de manière systématique l'impact qu'un risque peut avoir.

En premier lieu, l'importance de l'impact des risques identifiés au chapitre précédent doit être estimée en termes qualitatifs en rapport avec les critères d'évaluation du risque définis dans la politique de gestion des risques. Concrètement, il s'agit de transformer la description textuelle des conséquences de chaque risque dans une forme numérique au moyen des critères d'évaluation définis au préalable. Tous les critères doivent être évalués pour chaque risque. L'évaluation doit en outre être pondérée par l'importance du critère.

Exemple :

Considérant les critères d'évaluation suivants :

Rang	Critère	Bas (1)	Moyen (2)	Haut (3)
4	Réputation et confiance	La réputation n'est affectée que de manière réduite ; peu ou pas d'effort pour la rétablir.	La réputation est altérée de manière substantielle ; des efforts sont nécessaire pour la rétablir.	La réputation est altérée de manière irrévocable.
3	Finance	Augmentation de moins de 10% des coûts opérationnels annuels.	Augmentation des coûts opérationnels annuels entre 10% et 20%.	Augmentation de plus de 20% des coûts opérationnels annuels.
2	Légal	Le risque de recours n'augmente pas significativement par rapport aux autres canaux de vote.	Le risque de recours augmente significativement par rapport aux autres canaux.	Recours quasi certains.

1	Productivité	Augmentation de moins de 20% de la charge de travail des droits politique et du secteur informatique de la chancellerie d'état.	Augmentation de la charge de travail des droits politique et du secteur informatique de la chancellerie d'état comprise entre 20% et 50%.	Augmentation de plus de 50% de la charge de travail des droits politique et du secteur informatique de la chancellerie d'état.

L'analyse du risque donne :

Risque	**Conséquence**	**Critères**	**Score**
Un activiste dans un domaine pour lequel le résultat du scrutin peut avoir une influence se fait passer pour un réparateur d'imprimante et profite de son accès à l'infrastructure pour y installer une caméra lui permettant de voir les codes d'initialisation des cartes de légitimation.	La caméra n'est pas trouvée et l'attaquant a enregistré une grande quantité de codes d'initialisation. Il trouve sur les réseaux sociaux une partie des dates de naissance correspondantes et il les utilise pour saisir des votes. Certains électeurs étonnés de ne pouvoir utiliser leur matériel contactent la chancellerie d'état. Cette dernière suspend le canal de vote électronique et débute une enquête. Les médias sont alertés de l'affaire et en font leur gros titre, ce qui génère un gros effort de communication pour la chancellerie d'état. Des recours sont interjetés et aboutissent à l'annulation du scrutin.	Réputation et confiance	2 (Moyen) x 4 (rang) = 8
		Finance	2 (Moyen) x 3 (rang) = 6
		Légal	3 (Haut) x 2 (rang) = 6
		Productivité	1 (Bas) x 1 (rang) = 1
		Total	8 + 6 + 6 + 1 = 21

En sus du score de risque, il peut être opportun de prendre en compte la probabilité d'occurrence de ce dernier. Pour la définition de la probabilité d'occurrence, une période de trois ans (soit environ dix scrutins fédéraux) sera considérée. Les appréciations seront exprimées selon l'échelle suivante :

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

Comme il s'agit d'une approche systématique, si l'on a recours à la probabilité d'occurrence, elle doit être définie pour tous les risques et pas seulement pour certains risques choisis.

4.8 Evaluation des risques

Le score de risque obtenu à l'étape précédente, le cas échéant en combinaison avec la probabilité d'occurrence, doit ici être mis en relation avec la politique de gestion des risques. Il permet de prioriser les risques entre eux et d'identifier les risques qui nécessitent une action.

4.9 Traitement des risques

La politique de gestion des risques définit les règles de traitement des risques selon leur importance. De manière générale, un risque peut être :

- Accepté : aucune action
- Surveillé : mise en place de métriques et suivi de ces dernières

- Mitigé : mise en œuvre d'une ou plusieurs mesures visant la réduction de l'impact ou de la probabilité d'occurrence du risque
- Transféré : transfert du risque à un tiers par le biais d'une police d'assurance ou de clauses contractuelles

Bien que le canton reste responsable de l'ensemble des risques du scrutin, il peut en confier une partie du traitement à des tiers par l'établissement d'un contrat qui devient alors une mesure en soit, éventuellement accompagné par des mesures de contrôles (visites, rapport écrit régulier, etc.). Le risque résiduel résultant de ces mesures étant un manquement du tiers à ses obligations, l'inefficacité de mesures qu'il a prises ou son acceptation d'un risque.

Il peut arriver qu'un risque qui doit être mitigé selon les règles définies dans la politique de gestion des risques ne puisse effectivement l'être. Dans ce cas, l'exception doit être justifiée et explicitement acceptée par le service compétent au niveau cantonal au sens de la OVotE.

Les exigences de l'annexe à la OVotE offrent une série non-exhaustive de mesures de mitigation des risques. Les plus importantes sont mises en évidence dans le tableau ci-dessous :

Réf.	Description	Objectifs de sécurité concernés	Exigences annexe OVotE
13.3	Un logiciel malveillant modifie le suffrage sur la plate-forme de l'utilisateur.	Exactitude des résultats	2.5, 2.12, 4.3, 8.4, 8.5, 8.8, 8.11
13.4	Un attaquant externe détourne le suffrage au moyen d'un empoisonnement du cache DNS.	Exactitude des résultats	2.5, 4.3, 8.4, 8.5, 8.8, 8.10, 8.11
13.5	Un attaquant externe modifie le suffrage au moyen de la technique de « l'homme du milieu », ou « MITM ».	Exactitude des résultats	2.5, 2.12, 4.3, 8.4, 8.5, 8.8, 8.11, 15.2
13.6	Un attaquant externe envoie au moyen d'une attaque MITM des données corrompues qui sont nécessaires pour émettre le suffrage et qui proviennent du système en ligne (par ex. un fichier Javascript).	Exactitude des résultats	8.10, 10, 15.2
13.7	Un attaquant interne manipule le logiciel, qui n'enregistre alors plus les suffrages.	Exactitude des résultats	3.6, 3.7, 3.14, 14.1, 22.1, 22.3, 24.1, 24.3
13.8	Un attaquant interne modifie, supprime ou multiplie des suffrages.	Exactitude des résultats	2.6, 3.3, 3.14, 3.16, 5.2, 14.7, 22.1, 22.3
13.9	Un attaquant interne ajoute des suffrages dans l'urne électronique.	Exactitude des résultats	2.6, 3.3, 3.14, 3.16, 5.2, 14.7, 22.1, 22.3
13.10	Une organisation hostile pénètre dans le système pour fausser le résultat.	Exactitude des résultats	2.6, 3.3, 3.14, 3.16, 5.2, 14.1, 14.7, 15.2, 16.1, 16.2
13.11	Un attaquant interne copie du matériel de vote et l'utilise.	Exactitude des résultats	2.8, 3.10, 3.14, 4.9, 6.2, 6.3, 7.1, 22.1, 22.3, 22.5
13.12	Un attaquant externe utilise des méthodes relevant de l'ingénierie sociale pour détourner l'attention du votant des mesures de sécurité (vérifiabilité individuelle).	Exactitude des résultats	4.3, 8.3, 8.4, 8.11

Réf.	Description	Objectifs de sécurité concernés	Exigences annexe OVotE
13.13	Un attaquant externe pénètre électroniquement, physiquement ou au moyen de procédés d'ingénierie sociale dans l'infrastructure du canton et manipule les composants de configuration ou s'empare de données de sécurité.	Exactitude des résultats	3.8, 3.10, 3.14, 15.2, 15.3, 16.1, 16.2, 21.2, 21.3, 22.2, 22.3, 22.5
13.14	Un attaquant externe pénètre électroniquement, physiquement ou au moyen de procédés d'ingénierie sociale dans l'infrastructure de l'imprimerie et s'empare des codes des cartes de légitimation.	Exactitude des résultats	3.10, 3.14, 6.2, 6.3, 7.1, 7.5, 7.7, 16.1, 16.2, 18.3, 21.2, 21.3, 22.2, 22.3, 22.5
13.15	Un attaquant externe pénètre électroniquement, physiquement ou au moyen de procédés d'ingénierie sociale dans l'infrastructure de La Poste et s'empare de cartes de légitimation.	Exactitude des résultats	3.8, 7.8, 18.3, 21.2, 21.3, 23.5
13.16	Une erreur se produit dans la vérifiabilité individuelle.	Exactitude des résultats	17.1, 17.2, 17.3, 24.4, 25.13
13.17	Une erreur se produit dans la vérifiabilité universelle.	Exactitude des résultats	17.1, 17.2, 17.3, 24.4, 25.13
13.18	Un dispositif technique des vérificateurs comporte une erreur.	Exactitude des résultats	17.1, 17.2, 17.3, 24.4, 25.13
13.19	Une « porte dérobée » est introduite dans le système via une dépendance logicielle et est mise à profit par un attaquant externe pour accéder au système.	Exactitude des résultats Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés Accessibilité et capacité opérationnelle du vote électronique Protection contre les manipulations des informations destinées aux électeurs Pas d'usage abusif des preuves relatives au comportement de vote	3.8, 3.15, 3.16, 3.18, 14.1, 16.1, 16.2, 22.2, 22.4, 24.3
13.20	Un logiciel malveillant installé sur la plate-forme utilisateur envoie le suffrage à une organisation hostile.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	8.5, 8.6, 15.2
13.21	Le suffrage est détourné au moyen d'un empoisonnement du cache DNS.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	2.7, 8.10, 8.11
13.22	Un attaquant externe lit le suffrage au moyen d'une attaque MITM.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	2.7, 8.10, 8.11, 15.2
13.23	Un attaquant interne utilise la clef et déchiffre des suffrages non anonymisés.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	3.1, 3.10, 3.14, 12.1, 12.2, 12.3, 22.1, 22.3
13.24	Le secret du vote est violé lors de la vérification de l'exactitude du traitement et du dépouillement.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	2.7, 3.10, 3.13, 3.14, 8.14, 12.1

Réf.	Description	Objectifs de sécurité concernés	Exigences annexe OVotE
13.25	Un attaquant interne lit des suffrages de manière anticipée sans devoir les déchiffrer.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	2.7, 3.2, 3.8, 3.14, 12.2, 15.2, 15.3, 22.1, 22.3
13.26	Une organisation hostile pénètre dans le système pour violer le secret du vote ou pour établir des résultats partiels de manière anticipée.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	2.7, 3.2, 3.8, 3.14, 12.1, 12.2, 14.1, 15.2, 15.3, 16.1, 16.2, 22.2, 22.4
13.27	Une erreur dans le processus de chiffrement rend celui-ci inopérant ou réduit son efficacité.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	3.8, 15.4, 16.1, 24.4
13.28	Un attaquant interne manipule le logiciel et celui-ci divulgue les suffrages.	Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés	3.6, 3.7, 3.11, 3.15, 12.2, 24.3
13.29	Un logiciel malveillant installé sur l'ordinateur de l'électeur empêche ce dernier de voter.	Accessibilité et capacité opérationnelle du canal de vote	4.4, 8.1, 8.2, 8.3, 8.5, 8.8, 8.11
13.30	Une organisation hostile mène une attaque du type « déni de service » (DOS).	Accessibilité et capacité opérationnelle du canal de vote	14.1, 14.8
13.31	Un attaquant interne configure mal le système; le dépouillement ne peut pas se faire.	Accessibilité et capacité opérationnelle du canal de vote	3.6, 3.8, 3.10, 24.2
13.32	Un attaquant interne falsifie les preuves cryptographiques de la vérifiabilité universelle.	Accessibilité et capacité opérationnelle du canal de vote	2.11, 3.8, 3.14, 3.16, 14.1, 22.1, 22.3
13.33	Une défaillance technique du système fait que le système n'est pas disponible au moment du dépouillement.	Accessibilité et capacité opérationnelle du canal de vote	14.1, 25.8, 25.13
13.34	Un dispositif technique des vérificateurs ne fonctionne pas au moment du dépouillement.	Accessibilité et capacité opérationnelle du canal de vote	25.8, 25.13
13.35	Une organisation hostile pénètre dans le système pour en perturber l'exploitation, pour manipuler les informations destinées aux électeurs ou pour obtenir des preuves relatives au comportement de vote des électeurs.	Accessibilité et capacité opérationnelle du canal de vote Protection contre les manipulations des informations destinées aux électeurs Pas d'usage abusif des preuves relatives au comportement de vote	8.1, 8.2, 8.3, 8.4, 8.5, 12.1, 14.1, 15.2, 15.3, 16.1, 16.2, 22.2, 22.4
13.36	Un attaquant interne vole les données concernant les adresses des électeurs.	Protection des informations personnelles concernant les électeurs	3.10, 3.14, 5.1, 21.3, 22.1, 22.3
13.37	Un logiciel malveillant influence des électeurs pendant qu'ils se forgent une opinion.	Protection contre les manipulations des informations destinées aux électeurs	8.3, 8.5, 8.10, 8.11
13.38	Un attaquant interne manipule le site Internet d'information ou le portail de vote et sème la confusion dans l'esprit des électeurs.	Protection contre les manipulations des informations destinées aux électeurs	4.3, 8.2, 8.3, 8.5, 8.7, 8.10, 8.11, 14.1, 22.1, 22.3, 23.3

Réf.	Description	Objectifs de sécurité concernés	Exigences annexe OVotE
13.39	Un attaquant interne prescrit à des électeurs si et comment ils doivent voter. Après le déchiffrement, il trouve dans l'infrastructure des pièces justificatives prouvant que les électeurs se sont tenus aux instructions.	Pas d'usage abusif des preuves relatives au comportement de vote	3.10, 3.14, 11.4, 11.7, 12.1, 12.5, 15.2, 15.3, 22.1, 22.3
13.40	Un attaquant externe prescrit à des électeurs si et comment ils doivent voter et leur demande une pièce justificative prouvant qu'ils se sont tenus aux instructions.	Pas d'usage abusif des preuves relatives au comportement de vote	4.7, 4.8

Les mesures prévues dans les exigences légales peuvent ne pas être suffisantes. Il convient de les supplémenter d'autres mesures jusqu'à atteindre un niveau de risque suffisamment faible (art. 9 OVotE).

Malgré la prise de mesures de mitigation, le risque peut ne pas être réduit à zéro, soit parce que la mesure elle-même peut ne pas être à 100% efficace, soit parce qu'elle ne couvre qu'une partie du risque. Dans ce cas, le risque résiduel doit être clairement identifié et correspondre aux critères d'acceptabilité définis dans la politique de gestion des risques.

5 Risques liés au domaine politique et à l'administration

Outre les risques inhérents à l'exploitation des systèmes de vote électronique, il faut apprécier les risques liés au domaine politique et à l'administration, c'est-à-dire des risques qui n'ont, dans une large mesure, aucun rapport avec l'exploitation. Ces risques concernent le niveau cantonal et dans certains cas le niveau fédéral également. Le tableau suivant en présente un inventaire minimal :

Risque		Domaine
RPA-1	Une plainte est déposée contre un canton pour avoir exploité un système dont les mesures de sécurité sont insuffisantes.	Légal
RPA-2	La Confédération a autorisé l'utilisation d'un système dont les mesures de sécurité ne satisfont pas les exigences légales.	Légal
RPA-3	Des différends nuisent à la coopération entre les autorités et la Poste, de sorte que le vote électronique ne peut plus être développé ou est interrompu.	Finance
RPA-4	Une investigation d'une attaque contre le vote électronique ne peut être menée à bien faute de moyens techniques.	Réputation et confiance
RPA-5	Une attaque contre le vote électronique ne peut être poursuivie faute de moyens légaux.	Réputation et confiance
RPA-6	Une campagne de dénigrement du vote électronique est lancée sur les réseaux sociaux ou dans les médias. Celle-ci peut se baser sur des événements en lien avec le vote électronique à l'étranger, le supposé manque de contrôle public des processus de vote, de fausses allégations relatives aux mécanismes de la vérifiabilité ou une communication défaillante des autorités.	Réputation et confiance
RPA-7	Lors du dépouillement, il est constaté que les résultats du vote électronique ne vont pas dans le même sens que les autres canaux de vote.	Réputation et confiance
RPA-8	Les cantons manquent de ressources pour la mise en œuvre du vote électronique.	Finance
RPA-9	Une campagne d'achat de vote à large échelle est lancée par un groupe qui dispose d'une plateforme d'achat anonyme.	Réputation et confiance
RPA-10	Un incident de sécurité survient pendant la phase de vote et une réaction appropriée n'a pas lieu à temps.	Réputation et confiance

6 Rôle de la Chancellerie fédérale dans l’appréciation des risques

La Chancellerie fédérale établi sa propre appréciation des risques pour le projet vote électronique. Elle y considère les risques techniques à un niveau global de même que les risques liés au domaine politique et à l’administration. La situation des cantons et de la Poste y est prise en considération. Cette appréciation est transmise aux cantons qui peuvent l’utiliser dans l’établissement de leur propre appréciation des risques. Elle est également publiée sur le site de la Chancellerie fédérale.

La Chancellerie fédérale apporte volontiers son soutien aux cantons si ceux-ci ont des questions en rapport avec l’appréciation des risques.