REPUBLIQUE ET CANTON DE GENEVE
Chancellerie d'Etat
Direction du Support et des Opérations de Vote

CHANCELLERIE D'ETAT

DÉPARTEMENT DE LA SÉCURITÉ,
DE LA DIGITALISATION ET DE LA CULTURE
SERVICE INFORMATIQUE DE L'ENTITÉ NEUCHÂTELOISE

Directive sur la gestion des risques

Vote électronique

Auteur	**Direction du vote électronique (GE)** **Direction du vote électronique (NE)**
Date	09.06.2026
Version	1.0
Classification	Aucun

Contrôle des modifications

Version	Date	Description	Nom
0.9	10.06.2025	Version pour les auditeurs	Direction du vote électronique (GE)
0.91	16.12.2025	Modifications formelles	Direction du vote électronique (GE) Direction du vote électronique (NE)
0.99	17.04.2026	Modifications formelles	Direction du vote électronique (GE) Direction du vote électronique (NE)
1.0	09.06.2026	Modifications formelles	Direction du vote électronique (GE) Direction du vote électronique (NE)

Autorités de contrôle/de validation

Contrôle	Validation	Date
Vice-chancelière (NE)	Vice-chancelière (NE)	05.06.2026

Documents référencés

N°	Document	Version
[1]	Ordonnance de la ChF du 25 mai 2022 sur le vote électronique (OVotE, RS 161.116)	Version du 07.07.2022
[2]	« Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process » du Software Engineering Institute (SEI) https://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419	Version du 01.05.2007
[3]	Guide de la Chancellerie fédérale pour l'appréciation des risques du système du vote électronique de La Poste Suisse (PDF) https://www.bk.admin.ch/dam/bk/fr/dokumente/pore/Vote--lectronique/Guide%20de%20la%20ChF_Appr%C3%A9ciation%20des%20risques%20vote%20%C3%A9lectronique,%20octobre%202022.pdf.download.pdf/Guide%20de%20la%20ChF_Appr%C3%A9ciation%20des%20risques%20vote%20%C3%A9lectronique,%20octobre%202022.pdf	Version du 04.10.2022
[4]	Directive sur la sécurité de l'information	Version actuelle
[5]	Glossaire	Version actuelle

Table des matières

1 But du document

Le présent document porte sur la méthodologie d'appréciation et de gestion des risques dans le cadre du vote électronique.

2 Introduction

La présente directive constitue la base 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.

La directive fait l'objet d'une revue régulière afin de garantir son actualité.

2.1 Mesures selon l'OVotE

Les mesures prévues par l'ordonnance de la ChF sur le vote électronique (OVotE) sont considérées comme mises en œuvre dans le cadre de l'appréciation des risques. En cas d'éventuelles non-conformités, l'appréciation des risques est complétée par les risques correspondants.

Le guide de la Chancellerie fédérale (voir *le document de référence [3]*) répertorie les mesures permettant de répondre aux menaces (cf. *tableau au point 4.9 du guide*). L'analyse des risques réalisée par les cantons comprend l'ensemble des références correspondant aux menaces définies dans le guide, afin d'assurer la traçabilité entre les risques du canton et les mesures prévues par l'OVotE. Il peut être utile de s'y référer dans le cas où une mesure ne serait pas efficace.

3 Objectifs de sécurité

Les risques sont appréciés sous l'angle des objectifs de sécurité suivants (selon l'art. 4 OVotE) :

- Exactitude des résultats
- Garantie du secret du vote et impossibilité d'établir des résultats partiels anticipés
- Accessibilité et capacité opérationnelle du canal de vote
- Protection des informations personnelles concernant les électeurs
- Protection contre les manipulations des informations destinées aux électeurs
- Pas d'usage abusif des preuves relatives au comportement de vote

4 Processus et responsabilités

Le processus d'appréciation des risques implique l'établissement d'un inventaire des actifs informationnels (avec description dans des profils distincts conformément au *point 5.2*) et d'un portefeuille des risques (voir *point 5.3*). La direction du vote électronique est responsable de ce processus et agit en tant que propriétaire des risques répertoriés dans le portefeuille. Le propriétaire des risques est chargé de vérifier les risques à intervalles réguliers conformément aux directives et de s'assurer que les mesures sont mises en œuvre dans les délais impartis. La périodicité du processus est décrite au *point 4.1*.

Les propriétaires respectifs des actifs informationnels sont chargés de définir les exigences de sécurité de ces actifs et de veiller à ce que des stratégies de protection appropriées soient mises en place pour répondre à ces exigences.

4.1 Périodicité du processus

Le propriétaire des risques doit examiner régulièrement les risques existants et mettre à jour le portefeuille des risques en y intégrant les nouveaux risques identifiés. Cet examen a lieu au moins une fois par an. Un réexamen est également lancé en cas de changements organisationnels, technologiques ou procéduraux importants. Les risques classifiés « à surveiller » doivent être examinés avant chaque scrutin (voir *point 9.3*).

5 Méthodologie et composants

5.1 Mise en application de la méthode OCTAVE Allegro

Le canton applique la méthode OCTAVE Allegro du Software Engineering Institute (SEI) de la Carnegie Mellon University *(*voir l*e document de référence [2]*), qui a également servi de base à l'appréciation des risques dans le guide de la Chancellerie fédérale (voir *le document de référence [3]*).

Elle prévoit les étapes suivantes :

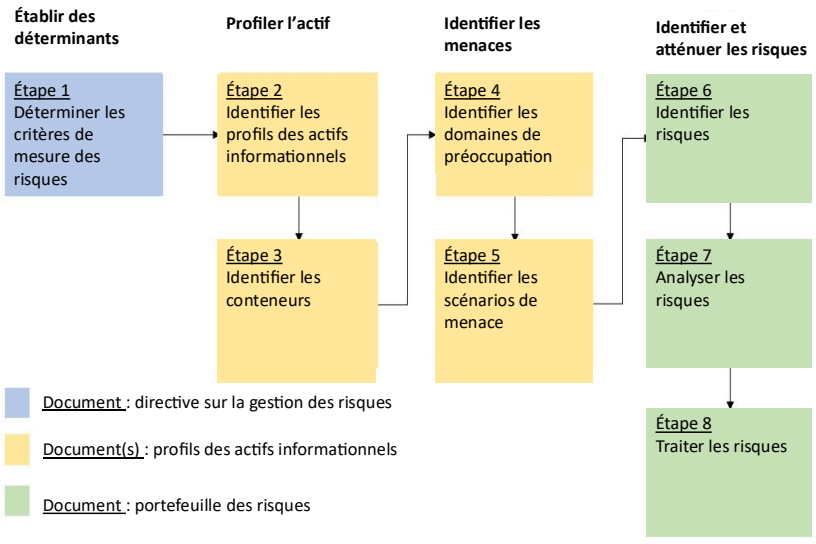

Illustration 1 : Etapes selon la méthode OCTAVE Allegro

Les critères de mesure des risques (**étape 1**) sont définis dans le présent document (voir *chapitre 8*). Les actifs informationnels et leurs conteneurs sont identifiés sur la base des processus clés définis.

L'élaboration des profils des actifs informationnels **(étape 2)** et des conteneurs correspondants **(étape 3)**, ainsi que l'identification des domaines problématiques **(étape 4)** et des scénarios de menace **(étape 5)**, sont réalisés dans les « profils des actifs informationnels » (voir *point 5.2*).

Les risques identifiés résultent des domaines problématiques et des scénarios de menace des profils (**étape 6**). L'analyse des risques (**étape 7**) et le traitement des risques (**étape 8**) identifiés sont effectués dans le « portefeuille des risques » (voir *point 5.3*).

5.2 Profils des actifs informationnels

Comme expliqué au *point 5.1*, les **étapes 2 à 5** sont traitées dans le cadre des profils des actifs informationnels. Un fichier Excel contenant les informations requises est établi pour chaque profil selon le modèle du SEI (voir *document de référence [2]*). Les profils doivent contenir les éléments suivants :

- Description des actifs informationnels
- Propriétaire des actifs informationnels
- Description et sélection des exigences de sécurité
- Liste et description des conteneurs
- Enumération des domaines problématiques et des scénarios de menace (y c. cartographie du risque)

L'identification préalable des actifs informationnels est expliquée au *chapitre 6*.

5.3 Portefeuille des risques

Conformément au *point 5.1*, les **étapes 6 à 8** sont traitées dans le portefeuille des risques. Pour ce qui est des menaces découlant des profils, les risques correspondants sont gérés, analysés et traités dans le portefeuille. Une feuille séparée contenant les informations prévues selon le modèle du SEI (voir *document de référence [2]*) doit être établie pour chaque risque au sein du portefeuille. Les fiches de risque contiennent les éléments suivants :

- Description de la menace (nature et impact du risque)
- Evaluation de la probabilité d'occurrence
- Description et évaluation de l'impact
- Calcul du score et du niveau de risque
- Description et sélection du traitement du risque

La description du risque est complétée par les objectifs de sécurité concernés (voir *chapitre 3*).

6 Identification des actifs informationnels et des conteneurs

Tous les actifs informationnels identifiés à l'aide des processus clés doivent être analysés. Sont concernés tous les actifs informationnels susceptibles de porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité des informations dans le cadre du vote électronique.

Les actifs informationnels peuvent comprendre des documents physiques ou électroniques, des applications et des bases de données, des personnes, des équipements informatiques, des infrastructures et des services/processus externalisés. L'identification des actifs informationnels implique également l'identification de leurs propriétaires (personnes ou unités organisationnelles responsables de chaque actif informationnel) et des conteneurs.

Les conteneurs sont les différents moyens qui permettent de traiter, d'enregistrer ou de transmettre les actifs informationnels. Ils peuvent être divisés en trois groupes :

- Environnement technique : appareils (p. ex. ordinateur), logiciels (p. ex. application informatique) ou connexions (p. ex. clé USB)
- Environnement physique : document physique, dossier physique, local, coffre-fort, etc.
- Environnement humain : personne ou groupe connaissant ou traitant des actifs informationnels

Les actifs informationnels et les conteneurs identifiés sont inscrits dans l'inventaire des actifs informationnels et analysés dans les profils des actifs informationnels (voir *point 5.2*).

La classification des actifs informationnels selon le document « Directive sur la sécurité de l'information » (voir *document de référence [4]*) et l'affectation des actifs informationnels identifiés à ceux du guide de la Chancellerie fédérale (voir *document de référence [3]*) sont réalisées dans le cadre de l'inventaire des actifs informationnels.

7 Identifications des risques

Il convient de déterminer, sur la base des actifs informationnels et des conteneurs qui leur sont associés, quels événements pourraient mettre en danger les exigences de protection de l'actif informationnel. L'identification des domaines problématiques et des scénarios de menace qui en découlent est effectuée pour chaque actif informationnel au moyen des profils des actifs informationnels (voir *point 5.2*), constituant la base de l'analyse des risques dans le portefeuille des risques (voir *point 5.3*).

8 Analyse des risques : critères d'appréciation des risques

Les critères de mesure des risques sont définis au début du processus et servent de base à l'appréciation des risques. Le propriétaire des risques et les propriétaires des actifs informationnels évaluent ensuite, à l'aide de l'échelle définie, les impacts et la probabilité d'occurrence de chaque scénario de risque.

L'appréciation des risques se fonde sur les directives du guide de la Chancellerie fédérale (voir *document de référence [3]*). Les chapitres suivants décrivent l'évaluation des critères et l'appréciation qui en découle.

8.1 Détermination de l'impact

Pour définir l'impact des risques, ces derniers sont appréciés en termes qualitatifs à l'aide de critères d'évaluation et traduits sous une forme numéraire.

Les critères d'évaluation suivants ont été définis pour l'analyse :

- **Réputation et confiance :** impact d'un risque sur la réputation ou la confiance dans le contexte du vote électronique
- **Finances :** impact financier d'un risque dans le contexte du vote électronique
- **Légal :** impact d'un risque sur le respect des exigences légales en matière de vote électronique
- **Productivité :** impact d'un risque sur la productivité opérationnelle

Tous les critères doivent être évalués pour chaque risque. L'impact est mesuré en deux étapes.

8.1.1 Etape 1 : identification du niveau de criticité

Le risque est d'abord apprécié sur la base de chaque critère d'évaluation, avec un classement du niveau de criticité : **bas, moyen ou haut.**

Le tableau suivant décrit, à l'aide d'exemples choisis, la classification du niveau de criticité pour chaque critère.

Domaine	**Bas**	**Moyen**	**Haut**
Critère : réputation et confiance	La réputation n'est affectée que de manière réduite ; peu ou pas d'efforts sont nécessaires pour la rétablir.	La réputation est altérée de manière substantielle ; des efforts sont nécessaire pour la rétablir.	La réputation est altérée de manière irrévocable.
	Echo dans les médias locaux.	Echo dans les médias régionaux.	Echo dans les médias nationaux.
Critère : finances	Les coûts opérationnels annuels augmentent de moins de 10 %.	Les coûts opérationnels annuels augmentent de 10 % à 20 %.	Les coûts opérationnels annuels augmentent de plus de 20 %.
Critère : légal	Le risque d'un recours susceptible d'aboutir n'augmente pas significativement par rapport aux autres canaux de vote.	Le risque d'un recours susceptible d'aboutir augmente significativement par rapport aux autres canaux.	Le risque d'un recours susceptible d'aboutir est quasi certain.

Domaine	**Bas**	**Moyen**	**Haut**
Critère : productivité	La charge de travail du secteur des droits politiques et du secteur informatique de la Chancellerie d'Etat augmente de moins de 20 %.	La charge de travail du secteur des droits politiques et du secteur informatique de la Chancellerie d'Etat augmente de 20 % à 50 %.	La charge de travail du secteur des droits politiques et du secteur informatique de la Chancellerie d'Etat augmente de plus de 50 %.

Tableau 1 : Exemples de classification du niveau de criticité des critères d'évaluation

8.1.2 Etape 2 : détermination du score de risque

L'impact de chaque risque est ensuite déterminé au moyen des formules suivantes :

- **Score du critère** = importance du critère multipliée par l'importance du niveau de criticité
- **Score de risque** = somme des scores de critère

Le tableau ci-après montre comment les critères d'évaluation et le niveau de criticité sont pondérés.

Pondération des critères d'évaluation	
Réputation et confiance	4
Finances	3
Légal	2
Productivité	1
Pondération du niveau de criticité	
Haut	3
Moyen	2
Bas	1

Tableau 2 : Pondération des critères et du niveau de criticité

8.2 Détermination de la probabilité d'occurrence

Une fois l'impact évalué, la probabilité d'occurrence de chaque scénario doit être appréciée. L'évaluation de la probabilité se base sur les gradations suivantes :

- **Haute (scénario hautement probable) :** il est fort probable qu'un incident se produise au cours de dix scrutins (probabilité supérieure à 30 %)
- **Moyenne (scénario probable) :** il est quasiment improbable qu'un incident se produise au cours de dix scrutins, mais il convient d'anticiper un éventuel incident (probabilité de l'ordre de 3 à 30 %)
- **Basse (scénario improbable) :** aucun incident ne se produira au cours de dix scrutins (probabilité inférieure à 3 %)

9 Traitement des risques

9.1 Détermination du niveau de risque

Le niveau de risque (voir *Tableau 3*) est déterminé en combinant le score de risque calculé au *point 8.1* avec la probabilité d'occurrence définie au *point 8.2*.

Le niveau de risque est calculé automatiquement dans la feuille de risque figurant dans le portefeuille (voir *point 5.3*) en fonction de la sélection effectuée.

Le niveau de risque permet de hiérarchiser les risques dans le cadre de leur traitement et d'identifier les risques qui nécessitent une action.

9.2 Critères d'acceptabilité des risques

La matrice suivante décrit comment les risques sont traités en fonction de leur niveau.

Impact	**21-30**	Risque significatif : à surveiller	Risque inacceptable : à atténuer	Risque inacceptable : à atténuer
	11-20	Risque faible : accepté	Risque significatif : à surveiller	Risque inacceptable : à atténuer
	10	Risque faible : accepté	Risque faible : accepté	Risque significatif : à surveiller
		Basse	**Moyenne**	**Haute**
		Probabilité		

Tableau 3 : Critères d'acceptabilité des risques

Le traitement de base des risques selon le niveau de risque est décrit au *point 9.3*. Le traitement des risques peut toutefois être défini de manière différente sur la base de décisions techniques. Un risque significatif donné pourra par exemple être défini comme devant être surveillé, mais aussi atténué.

9.3 Traitement des risques

Le traitement des risques est mis en œuvre par la direction du vote électronique à l'aide du portefeuille des risques (voir *point 5.3*). Les différentes options permettant de traiter les risques sont expliquées dans le tableau ci-après.

Accepté	Aucune action n'est nécessaire. L'évaluation doit toutefois faire l'objet d'un réexamen régulier (chaque année ou en cas de modifications organisationnelles, technologiques ou procédurales importantes).
A surveiller	Les risques sont surveillés régulièrement. Un examen est effectué avant chaque scrutin.
A atténuer	Une ou plusieurs mesures visant à réduire l'impact ou la probabilité d'occurrence du risque sont mises en œuvre. Le risque résiduel est ensuite à nouveau identifié et évalué. Si un risque ne peut être atténué efficacement, l'exception doit être justifiée et approuvée expressément par la direction de l'autorité supérieure VE.
Transféré	Les risques sont supportés par un tiers, qui réduit l'ampleur des dommages pour le canton (p. ex. couverture des dommages financiers par une assurance). Le portefeuille des risques ne contient aucun risque de cette catégorie.

Tableau 4 : Options de traitement des risques

Lorsqu'un risque concerne un fournisseur du canton, ce dernier peut lui confier la mise en œuvre des mesures. Le canton informe les fournisseurs de tous les risques les concernant et contrôle la mise en œuvre des mesures éventuelles.

10 Liste des illustrations

11 Liste des tableaux