Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Sektion Politische Rechte

1. März 2023

Prozess Risikomanagement Vote électronique der Bundeskanzlei

Inhaltsverzeichnis

1 Einleitung

1.1 Ausgangslage

Die Ausprägung der Risiken hängt nicht allein davon ab, ob und wie die in der Verordnung der Bundeskanzlei (BK) über die elektronische Stimmabgabe (VEleS; SR 161.116) definierten Anforderungen erfüllt werden. Sie hängt ebenfalls von der aktuellen Bedrohungslage ab. Zusätzlich können sicherheitsrelevante Vorfälle, die beim Betrieb der Systeme gehäuft auftreten, oder neue Erkenntnisse zur allgemeinen Bedrohungslage zu einer veränderten Einschätzung der Risikolage führen. Diese Überlegungen sind in die VEleS eingeflossen: Die Kantone müssen die Risiken, die mit der elektronischen Stimmabgabe in Zusammenhang stehen, fortlaufend beurteilen (Art. 4 VEleS). Falls die Risiken trotz der ergriffenen Massnahmen nicht hinreichend gering sind, müssen zusätzliche Massnahmen zur Risikominimierung ergriffen werden (Art. 9 VEleS). Die Kantone müssen der BK vor jedem Urnengang, bei dem E-Voting eingesetzt werden soll, aktuelle Risikobeurteilungen einreichen (Art. 15 Abs. 1 Bst. a VEleS). Die BK überprüft die Plausibilität der Beurteilung anhand der umgesetzten Massnahmen und versichert sich, dass die Risiken hinreichend gering sind. Gestützt darauf entscheidet die BK, ob sie die Durchführung eines Versuchs mit der elektronischen Stimmabgabe zulässt.

Ob die Voraussetzungen für die Zulassung von E-Voting-Versuchen effektiv erfüllt sind, hängt demnach nicht ausschliesslich von der Erfüllung der technischen und organisatorischen Anforderungen ab. Vielmehr steht das übergeordnete Ziel im Vordergrund, dass die in den Rechtsgrundlagen definierten Sicherheitsziele (vgl. Art 4 Abs. 3 VEleS) so weit wie möglich erreicht werden und dass die Risiken, die die Erreichung dieser Sicherheitsziele bedrohen, bekannt sind, evaluiert und durch geeignete Massnahmen gemindert werden. Die Risiken müssen hinreichend gering sein. Einem verantwortungsbewussten Umgang mit Risiken liegt naturgemäss ein wirksames Risikomanagement sowohl auf Bundes- als auch auf Kantonsebene zugrunde.

1.2 Ziele

Mit dem Risikomanagement im Bereich von Vote électronique verfolgt die BK die folgenden Ziele:

- Sowohl auf der Steuerungs- als auch auf operativer Ebene besteht ein verantwortungsbewusster Umgang mit Risiken, die mit Vote électronique in Zusammenhang stehen.
- Die mit Vote électronique in Zusammenhang stehenden Risiken bewegen sich gemäss den definierten Bewertungskriterien auf einem akzeptablen Niveau.
- Die BK und die Kantone kennen die mit Vote électronique in Zusammenhang stehenden Risiken. Die auf der Steuerungs- und auf der operativer Ebene verantwortlichen Personen haben Kenntnis über die für sie relevanten Informationen.
- Die BK und die Kantone reagieren wirksam und konsistent auf risikobezogene Ereignisse.

1.3 Anwendungsbereich

Das vorliegende Dokument bezieht sich ausschliesslich auf das Risikomanagement der BK im Rahmen des Projekts Vote électronique. Die Kantone und ihre Dienstleister im Bereich von E-Voting verfügen über eigene Risikomanagementprozesse. Die BK setzt für ihr Risikomanagement einen eigenen Risikomanagementprozess um, der nach den Vorgaben des Bundes erarbeitet wurde.[1] Die im vorliegenden Dokument dargestellten Risiken werden in aggregierter Form in diesen Prozess integriert.

1.4 Lebenszyklus

Das vorliegende Dokument wird von der BK erstellt und auf dem neusten Stand gehalten. Dabei kann sie sich von Expertinnen und Experten aus der Bundesverwaltung, Wissenschaft und Industrie unterstützen lassen.

Das vorliegende Dokument wird jährlich und entsprechend dem jeweiligen Wissensstand überarbeitet.

---

[1] www.efv.admin.ch > Themen > Finanzpolitik, Grundlagen > Risiko- und Versicherungspolitik.

2 Zuständigkeiten bei der Durchführung von eidgenössischen Urnengängen

2.1 Zuständigkeiten der Kantone

Die Durchführung von eidgenössischen Wahlen und Abstimmungen liegt im Zuständigkeitsbereich der Kantone. Demnach sind die Kantone auch für den korrekten Ablauf der Urnengänge mit der elektronischen Stimmabgabe zuständig (Art. 14 VEleS). Im Rahmen dieser Zuständigkeit erstellen sie Risikobeurteilungen, die sich auf die Durchführung von Versuchen mit der elektronischen Stimmabgabe bezieht (Art. 4 VEleS). Die Risikobeurteilungen der Kantone und gegebenenfalls ihrer Dienstleister dienen dazu, aufzuzeigen, dass sich die Risiken auf einem hinreichend geringen Niveau bewegen und dass die Kantone die Risiken angemessen kontrollieren.

2.2 Zuständigkeiten der Bundeskanzlei

Im Bereich von Vote électronique ist die BK für die folgenden Aspekte zuständig:

- **Allgemeine Aufgaben:**
  - Die BK sorgt dafür, dass die Volksrechte im Rahmen von Bundesverfassung und Gesetzgebung über die politischen Rechte wahrgenommen werden können und dass alle eidgenössischen Abstimmungen und Wahlen korrekt durchgeführt werden (Art. 1 Abs. 4 Bst. a Organisationsverordnung für die BK, OV-BK, SR 172.210.10)
  - Vorbereitung und Vollzug des Bundesgesetzes über die politischen Rechte (BPR; SR 161.1) und der Verordnung über die politischen Rechte (VPR; SR 161.11)
  - Definition und Umsetzung von Zulassungsanforderungen zur elektronischen Stimmabgabe in der Verordnung der BK (VEleS)
  - Beobachten von politischen, technischen und rechtlichen Entwicklungen im Bereich der elektronischen Stimmabgabe und Vorsehen von entsprechenden Massnahmen (insbes. zur Sicherstellung der Sicherheit der Systeme und einer wirksamen Kontrolle und Aufsicht, zur Stärkung der Transparenz und des Vertrauens sowie zur stärkeren Vernetzung mit der Wissenschaft)
  - Einbezug der Öffentlichkeit und von Fachkreisen (Art. 27*l* VPR)
  - Information der Öffentlichkeit zu E-Voting im Allgemeinen, zu den bundesrechtlichen Anforderungen, zum Stand des Projektes Vote électronique und zu Entwicklungen mit nationaler und internationaler Bedeutung
  - Die BK stellt eine wissenschaftliche Begleitung der Versuche mit der elektronischen Stimmabgabe sicher (Art. 27*o* Abs. 2 und 3 VPR)

- **Operative und fachliche Leitung des Projektes Vote électronique:**
  - Koordination der kantonalen Projekte
  - Verwaltung der Gremien des Projekts Vote électronique
  - Definition von Massnahmen und Umsetzung beschlossener Massnahmen in der Zuständigkeit der BK
  - Zusammenarbeit mit bundesinternen Stellen und Beizug unabhängiger Fachpersonen bei der Erfüllung der Aufgaben der BK (Art. 27*o* Abs. 1 VPR)
  - Einbettung und Umsetzung des Projekts als Teil der E-Government-Strategie Schweiz, entsprechende Zusammenarbeit mit der Digitalen Verwaltung Schweiz, Vergabe und Begleitung von mitfinanzierten Projekten

- **Bewilligung und Zulassung von Versuchen mit der elektronischen Stimmabgabe:**
  - Prüfung, ob die bundesrechtlichen Anforderungen für die Erteilung von Grundbewilligungen und Zulassungen erfüllt sind (inkl. Durchführung unabhängiger Überprüfung der Systeme und

deren Betrieb, Publikation von Prüfberichten und Beurteilung von Risiken auf nationaler Ebene)

- Genehmigung oder Ablehnung von Zulassungsgesuchen
- Behandlung der Gesuche der Kantone und Antragstellung an den Bundesrat für die Genehmigung oder Ablehnung von Grundbewilligungsgesuchen

Die BK erstellt im Rahmen ihrer Zuständigkeiten eine Risikobeurteilung, die sich auf die Prozesse und Tätigkeiten stützt, die den oben genannten Aufgaben zugrunde liegen (vgl. Kapitel 4.1).

3 Risikomanagementprozess

Die Identifizierung, die Evaluation und die Behandlung der Risiken erfolgen nach den in den folgenden Kapiteln definierten Kriterien. Diese wurden grösstenteils aus der Methode OCTAVE Allegro übernommen. Diese Methodik bildet auch die Grundlage für den Leitfaden der BK zu den Risikobeurteilungen.[2] Indem alle Akteure eine gemeinsame Grundlage verwenden, können die Risikobeurteilungen besser aufeinander abgestimmt und es kann ein besseres Verständnis der Risiken durch die verschiedenen Akteure gewährleistet werden.

Die identifizierten, evaluierten und behandelten Risiken werden anschliessend in aggregierter Form in den Risikomanagementprozess des Bundes aufgenommen.

3.1 Identifizierung

Zur Identifizierung der Risiken müssen zunächst die Kernprozesse der BK in Bezug auf Vote électronique sowie die Elemente, die für eine korrekte Durchführung dieser Prozesse erforderlich sind, identifiziert werden. Diese Elemente werden in den folgenden Teilen des vorliegenden Dokuments als «Ressourcen» bezeichnet. Für jede dieser Ressourcen erfolgt anschliessend eine Analyse der Bedrohungen, die sie gefährden und die das Erreichen der Sicherheitsziele beeinträchtigen könnten. Die identifizierten Bedrohungen mit relevanten Auswirkungen auf die Sicherheitsziele, werden schliesslich in einer Liste von Risiken zusammengefasst.

3.2 Analyse und Evaluation

Für jedes Risiko werden die Folgen des Eintretens analysiert. Diese Folgen werden ohne das Ergreifen von Massnahmen zur Risikominimierung betrachtet. Sie entsprechen dem worst-case-Szenario, zu dem das Risiko führen könnte, und werden in Textform dargestellt. Anschliessend müssen sie anhand der Kriterien zur Risikomessung evaluiert werden. Diese Kriterien bestehen aus verschiedenen qualitativen Messungen, mit denen die Auswirkungen eines Risikos auf die Zielsetzung der BK beurteilt werden können. Die Kriterien müssen konsistent sein und die Sichtweise der BK wiedergeben, damit kohärente Entscheidungen zur Risikominimierung getroffen werden können. Zudem werden sie anhand ihrer Bedeutung für die Erfüllung des Auftrags der BK gewichtet.

Die Kriterien der BK zur Risikomessung im Bereich Vote électronique werden in der folgenden Tabelle aufgeführt. Sind für einen Bereich mehrere Zeilen definiert, gilt die Auflage mit dem höchsten Schweregrad.

Wirkungsbereich	**Kriterien zur Risikomessung**			
	Tief (1)	**Mittel (2)**	**Hoch (3)**	**Gewicht**
Reputation und Vertrauen	Die Glaubwürdigkeit der Bundesbehörden ist nicht oder nur geringfügig beeinträchtigt.	Die Glaubwürdigkeit der Bundesbehörden ist mittelschwer beeinträchtigt.	Die Glaubwürdigkeit der Bundesbehörden ist schwer beeinträchtigt.	5

[2] www.bk.admin.ch > Politische Rechte > E-Voting > Bundesrechtliche Anforderungen.

Wirkungsbereich	Kriterien zur Risikomessung			
	Tief (1)	**Mittel (2)**	**Hoch (3)**	**Gewicht**
	Die Korrektheit der Ergebnisse der Urnengänge wird nicht in Frage gestellt.	Die Korrektheit der Ergebnisse der Urnengänge wird geringfügig in Frage gestellt.	Die Korrektheit der Ergebnisse der Urnengänge wird weitgehend in Frage gestellt.	
Rechtliches	Der Bundesrat kann die Ergebnisse der Urnengänge ohne Verzögerung erwahren.	Der Bundesrat kann die Ergebnisse der Urnengänge mit Verzögerung erwahren.	Der Bundesrat kann die Ergebnisse der Urnengänge nicht erwahren.	5
	Die Integrität des Urnengangs ist intakt.	Es fand eine isolierte Manipulation von Stimmen statt.	Es fand eine systematische Manipulation von Stimmen statt.	
	Das Stimmgeheimnis wurde nicht verletzt.	Das Stimmgeheimnis wurde vereinzelt verletzt.	Das Stimmgeheimnis wurde systematisch verletzt.	
Kontinuität des elektronischen Stimmkanals	Der weitere Einsatz von E-Voting wird nicht oder nur geringfügig in Frage gestellt.	Der weitere Einsatz von E-Voting wird ernsthaft in Frage gestellt.	E-Voting muss mit hoher Wahrscheinlichkeit eingestellt werden.	3
Finanzen	Die wiederkehrenden Kosten für das Projekt Vote électronique der BK steigen nicht an.	Die wiederkehrenden Kosten für das Projekt Vote électronique der BK steigen moderat an.	Die wiederkehrenden Kosten für das Projekt Vote électronique der BK steigen signifikant an.	3
	Es gibt keinen oder nur einen moderaten einmaligen Kostenanstieg.	Es gibt einen signifikanten einmaligen Kostenanstieg.		
Produktivität	Der Arbeitsaufwand nimmt nicht oder nur punktuell und mässig zu.	Der Arbeitsaufwand nimmt entweder dauerhaft, aber nur mässig, oder punktuell, aber deutlich zu.	Der Arbeitsaufwand nimmt dauerhaft und deutlich zu.	1

Die Eintretenswahrscheinlichkeit der Risiken wird anschliessend anhand einer Skala eingeschätzt, die sich auf einen Zeitraum von drei Jahren bezieht (rund 10 Urnengänge) und die aufgrund subjektiver Einschätzungen erstellt wird. Diese Skala wird bei Bedarf aufgrund von gewonnenen Erkenntnissen angepasst.

- Hoch (3): wahrscheinliches Szenario: Es ist sehr wahrscheinlich, dass ein solches Ereignis innerhalb von zehn Urnengängen eintritt (Wahrscheinlichkeit höher als 30 %).
- Mittel (2): mögliches Szenario: Die Wahrscheinlichkeit, dass ein solches Ereignis innerhalb von zehn Urnengängen eintritt, liegt in der Regel bei null, dennoch muss ein mögliches Ereignis antizipiert werden (Wahrscheinlichkeit zwischen 3 und 30 %).
- Tief (1): unwahrscheinliches Szenario: Innerhalb von zehn Urnengängen tritt kein solches Ereignis ein (Wahrscheinlichkeit weniger als 3 %).

Diese Wahrscheinlichkeit gilt nur für das Risiko bzw. für das Ereignis, welches das Risiko ausmacht. Sie gilt nicht für das Szenario, das die Folgen bei einem Eintreten des Risikos beschreibt.

3.3 Risikobehandlung (Umgang)

Die BK entscheidet anhand des Scores und der Eintretenswahrscheinlichkeit, wie mit dem Risiko umzugehen ist. Dazu verfügt die BK über die folgenden Möglichkeiten:

Wahrscheinlichkeit	**Score**		
	32 – 49	**22 – 31**	**17 – 21**
Hoch	Minimieren	Minimieren	Minimieren Beobachten
Mittel	Minimieren	Minimieren Beobachten	Minimieren Beobachten Akzeptieren
Tief	Minimieren Beobachten	Minimieren Beobachten Akzeptieren	Minimieren Beobachten Akzeptieren

3.4 Restrisiken

Nachdem der Arbeitsschritt zur Risikobehandlung abgeschlossen ist, sind die Restrisiken zu identifizieren und zu evaluieren. Damit der elektronische Stimmkanal eingesetzt werden kann, müssen die Restrisiken von der BK explizit akzeptiert werden.

3.5 Überwachung und Überprüfung von Risiken

Die BK überprüft die Risiken mindestens jährlich. Dabei müssen alle relevanten Ereignisse berücksichtigt werden, die seit der letzten Überprüfung eingetreten sind. Diese Ereignisse können auf politischer Ebene (z.B. parlamentarische Vorstösse oder neue Regulierung) eingetreten, sicherheitsrelevant (z.B. Sicherheitslücken, die das System oder Teile seiner Infrastruktur betreffen) oder technischer Natur (z.B. Entwicklung neuer Technologien mit positivem oder negativem Einfluss auf die Sicherheit von E-Voting) sein.

Zusätzlich zur jährlichen Überprüfung werden Risiken identifiziert, evaluiert und gegebenenfalls behandelt, die sich spezifisch aus einzelnen Urnengängen ergeben können. Dabei sind die seit der letzten Überprüfung eingetretenen Ereignisse sowie die besonderen Umstände des spezifischen Urnengangs zu berücksichtigen.

3.6 Dokumentation

Das Resultat aller Arbeitsschritte des Risikomanagementprozesses muss in der Risikobeurteilung Vote électronique der BK dokumentiert werden. Die Risikobeurteilung ist von einer kompetenten Stelle zu überprüfen und von der BK zu genehmigen. Sie wird anschliessend auf der Webseite der BK publiziert und den betroffenen Kantonen zugestellt.

3.7 Integration der mit E-Voting verbundenen Risiken in das Risikomanagement der BK und des Bundes

Für den Umgang mit Risiken in ihrem Zuständigkeitsbereich verfügt die BK über einen eigenen Risikomanagementprozess, der nach den Vorgaben für den Risikomanagementprozess des Bundes erstellt wurde. Darin werden die Risiken systematisch identifiziert, dokumentiert und evaluiert. Die Risiken, die im vorliegenden Dokument dargestellt werden, werden in einer für die BK aggregierten Form übernommen. In diesem Rahmen werden sie von der für das Risikomanagement der BK zuständigen Stelle überprüft.

4 Zentrale Elemente für die Risikobeurteilung Vote électronique der BK

4.1 Kernprozesse und -aktivitäten

Die Zuständigkeiten der BK im Bereich von Vote électronique (vgl. Kapitel 2.2) werden mit den folgenden Prozessen und Aktivitäten erfüllt:

1. [Rechtsgrundlagen] Erarbeiten und Aufrechterhalten der rechtlichen Grundlagen für die Versuche mit Vote électronique
   - Beobachten der technologischen, soziologischen und rechtlichen Entwicklungen im Bereich von Vote électronique
   - Beobachten von Entwicklungen im Bereich der Informationssicherheit
   - Revision von VPR und VEleS
2. [Bewilligung] Zulassung und Bewilligung für einen Kanton für den Einsatz eines E-Voting-Systems
   - Sicherstellen der unabhängigen Überprüfung des Systems und / oder der Kantone
   - Umgang mit Nichtkonformitäten
   - Prüfen, ob die Zulassungsvoraussetzungen erfüllt sind
   - Entscheid zur Erteilung oder Verweigerung der Zulassung
   - Vorbereiten von Bundesratsentscheiden zu beantragten Grundbewilligungen
3. [Überwachung] Überwachen der ordnungsgemässen Umsetzung der Versuchsphase inkl. der korrekten Durchführung der Urnengänge
   - Definieren, Erheben und Publizieren von Kennzahlen zu Versuchen, die mit der elektronischen Stimmabgabe durchgeführt werden (z.B. Beteiligung über den elektronischen Stimmkanal, Anzahl Stimmen pro Abstimmungsfrage bzw. kandidierende Person oder Liste)
   - Überwachen und Begleiten eines ordnungsgemässen Umgangs mit Hinweisen zu Unregelmässigkeiten oder Mängeln, die während der Durchführung von eidgenössischen Urnengängen eingehen
   - Begleitung und Unterstützung der kantonalen Projekte
4. [Kommunikation] Ausarbeiten und Umsetzen einer transparenten und sachlichen Kommunikationsstrategie
5. [Begleitung] Sicherstellen einer wissenschaftlichen Begleitung für die Versuche mit der elektronischen Stimmabgabe
   - Etablieren eines Dialogs mit der Wissenschaft
   - Untersuchen der Versuche, um Verbesserungspotenzial zu identifizieren (z.B. Barrierefreiheit, Vertrauen und Akzeptanz durch die Stimmberechtigten, Stärkung der Verifizierbarkeit)
   - Analysieren, Terminieren und Umsetzen von Verbesserungsmassnahmen
6. [Risiken] Risikomanagement der BK in Bezug auf Vote électronique
   - Erarbeiten und Aufrechterhalten eines Leitfadens für die Risikobeurteilungen
   - Erstellen einer Risikobeurteilung sowie laufende Überprüfung und Anpassung bei Bedarf
   - Sicherstellen einer Überwachung der Bedrohungen
7. [Krisen] Bewältigung von Krisen, die im Zusammenhang mit Vote électronique stehen und denen eine nationale Bedeutung zukommt
   - Erarbeiten und Aufrechterhalten einer gemeinsamen Krisenvereinbarung
   - Erarbeiten und laufendes Aktualisieren von Krisenszenarien
   - Organisation und Durchführung von Krisenübungen

4.2 Ressourcenkatalog

Im Zusammenhang mit der Risikobeurteilung werden Ressourcen als die Gesamtheit der materiellen und immateriellen Elemente verstanden, die von der BK benötigt werden, um die im vorherigen Kapitel definierten Kernprozesse und -aktivitäten umzusetzen. Die folgende Tabelle enthält eine Liste dieser Ressourcen mit Verweisen auf die von ihnen abhängigen Prozesse sowie Begründungen, weshalb sie in die Risikobeurteilung einbezogen werden.

Ressource	Davon abhängige Prozesse	Weshalb ist diese Ressource wichtig?	Auswirkungen einer Beeinträchtigung dieser Ressource	Sicherheitsanforderungen
Ergebnisse eidg. Urnengänge	Überwachung Kommunikation	Die Ergebnisse der Urnengänge müssen dem Willen der Stimmenden entsprechen und verfügbar sein.	Vertrauensverlust ins politische System und den elektronischen Stimmkanal.	Integrität Verfügbarkeit
Vertrauen der Stimmberechtigten	Rechtsgrundlagen Kommunikation	Ohne Vertrauen in den elektronischen Stimmkanal kann dieser nicht genutzt werden.	Möglicherweise wird der elektronische Stimmkanal eingestellt.	Verfügbarkeit
VPR und VEleS	Rechtsgrundlagen Bewilligung	Für die Durchführung von Versuchen ist eine Rechtsgrundlage notwendig. In den Rechtsgrundlagen werden die Sicherheitsanforderungen festgelegt.	Wenn die Rechtsgrundlagen ein zu tiefes Sicherheitsniveau festlegen, könnte ein System bewilligt werden, das zu wenig Sicherheit bietet.	Integrität
Unabhängige und kompetente Expertinnen und Experten	Rechtsgrundlagen Bewilligung Kommunikation Begleitung Risiken Krisen	Unabhängige Expertinnen und Experten sind bei der Überprüfung der Systeme, der Verbesserung der verfügbaren und empfohlenen Technologien, der Begleitung der Versuche sowie für die öffentliche Debatte notwendig.	Bei einem Mangel an kompetenten Expertinnen und Experten könnten sich Bewilligungsverfahren verzögern, die rechtlichen Anforderungen nicht mehr angemessen sein und keine sachliche und objektive Debatte mehr stattfinden.	Verfügbarkeit
Kantone mit E-Voting-Versuchen	Rechtsgrundlagen Bewilligung Überwachung Kommunikation Risiken Krisen	Kantone, die E-Voting-Versuche durchführen, sammeln Erfahrungen und Informationen, die notwendig sind, um Schlussfolgerungen aus den Versuchen zu ziehen und den elektronischen Stimmkanal weiterzuentwickeln. Ausserdem spielen sie eine wichtige Rolle beim Aufbau von Vertrauen der Stimmberechtigten und bei der Förderung des Einbezugs der Öffentlichkeit.	Wenn kein Kanton bereit ist, E-Voting-Versuche durchzuführen, kann der elektronische Stimmkanal nicht weiterentwickelt werden.	Verfügbarkeit

Ressource	Davon abhängige Prozesse	Weshalb ist diese Ressource wichtig?	Auswirkungen einer Beeinträchtigung dieser Ressource	Sicherheitsanforderungen
Systemanbieter	Bewilligung Überwachung Kommunikation Risiken Krisen	Die Verfügbarkeit eines zuverlässigen Systemanbieters und die Massnahmen, die er für die Sicherheit des Systems ergreift, sind entscheidend für das Vertrauen der Stimmberechtigten.	Wenn kein Systemanbieter existiert, der die Anforderungen der BK erfüllen kann, können keine Versuche mit der elektronischen Stimmabgabe durchgeführt und E-Voting kann nicht weiterentwickelt werden. Zudem kann ein wenig überzeugender Anbieter das Vertrauen der Stimmberechtigten negativ beeinflussen.	Verfügbarkeit
Vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe	Bewilligung Überwachung Kommunikation Risiken Krisen	Die Ergebnisse der Urnengänge müssen dem Willen der Stimmenden entsprechen und verfügbar sein. Die BK stellt eine wirksame Überwachung der Versuche sicher, die in Übereinstimmung mit den bundesrechtlichen Anforderungen durchgeführt werden. Dazu ist sie darauf angewiesen, dass die Urnengänge mit der elektronischen Stimmabgabe ordnungsgemäss durchgeführt und überprüft werden.	Wird ein Urnengang manipuliert, könnte dies zu einem Vertrauensverlust in das politische System und die Behörden führen. Beschwerden gegen die Ergebnisse des Urnengangs könnten erfolgen und zu einer Wiederholung des Urnengangs führen.	Integrität Vertraulichkeit Verfügbarkeit

4.3 Risikokatalog

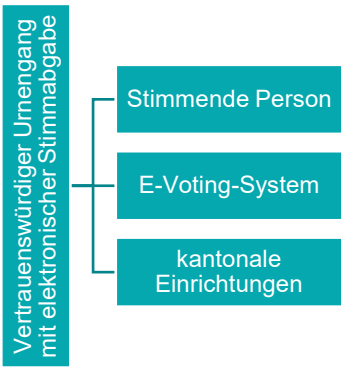
Der Katalog der auf der Grundlage der im vorherigen Kapitel dargestellten Ressourcen identifizierten Risiken, wird in der Risikobeurteilung Vote électronique der BK aufgeführt.

5 Beispiel für die Umsetzung des Risikomanagementprozesses

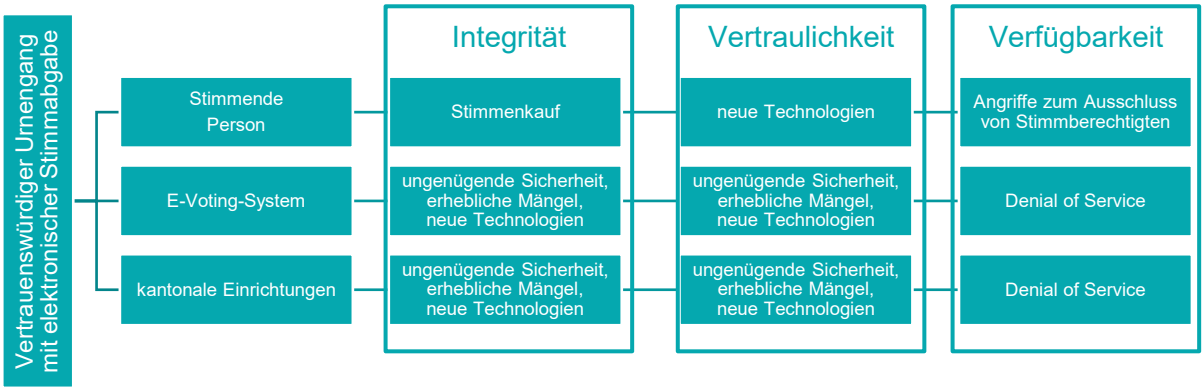
Das in diesem Kapitel dargestellte Beispiel soll den im vorliegenden Dokument beschriebenen Prozess veranschaulichen. Das Beispiel bildet keinen tatsächlichen Anwendungsfall ab.

5.1 Identifizierung

Bei der im vorliegenden Dokument beschriebenen Methode wird zunächst von einer Ressource ausgegangen und es werden die Elemente bestimmt, die einen Einfluss auf diese Ressource und deren Sicherheitsanforderungen (Integrität, Vertraulichkeit, Verfügbarkeit) haben können. Die Sicherheitsanforderungen werden insofern berücksichtigt, als dass sie der Erreichung der Sicherheitsziele (vgl. Art. 4 Abs. 3 VEleS) dienen. Für die Ressource «vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe» ergibt dies:



Anschliessend wird im Hinblick auf diese Elemente ermittelt, was die für die betroffene Ressource geltenden Sicherheitsanforderungen beeinträchtigen könnte. So entsteht eine Aufstellung der Bedrohungen:



Sicherheitsziele (Art. 4 Abs. 3 VEleS)

- *a. Korrektheit des Ergebnisses*
- *c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals*
- *e. Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen*

- *b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen*
- *d. Schutz der persönlichen Informationen über die stimmberechtigten Personen*
- *f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten*

- *a. Korrektheit des Ergebnisses*
- *c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals*

Nun können die Bedrohungen in Form von Risiken beschrieben werden, die ein mögliches Szenario für das Eintreten der Bedrohung darstellen. Die Risiken werden eindeutig identifiziert, damit sie im gesamten Risikobeurteilungsprozess referenziert werden können. Im vorliegenden Beispiel wird nur ein einziges Risiko abgebildet:

Identifikation	Beschreibung	Ressourcen
Risiko_1	Der Bund hat den Einsatz eines Systems bewilligt, das die bundesrechtlichen Sicherheitsanforderungen nicht erfüllt.	Vertrauenswürdiger Urnengang mit elektronischer Stimmabgabe
Sicherheitsziele (Art. 4 Abs. 3 VEleS)		
a. Korrektheit des Ergebnisses b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals d. Schutz der persönlichen Informationen über die stimmberechtigten Personen e. Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten		

5.2 Analyse und Evaluation

Ausgehend der für das Risiko identifizierten und dokumentierten Bedrohung, wird nun deren Eintretenswahrscheinlichkeit eingeschätzt. Dazu wird die in Kapitel 3.2 definierte Bewertungsskala verwendet. Diese Einschätzung bezieht sich auf den Zustand, der sich vor der Umsetzung von allfälligen Massnahmen ergibt. Im vorliegenden Beispiel wird die Wahrscheinlichkeit auf «mittel» geschätzt, denn obwohl es unwahrscheinlich ist, dass der Bund ein System bewilligt, das die bundesrechtlichen Anforderungen nicht erfüllt, muss dieser Fall antizipiert werden.

Risiko_1 Zulassung eines mangelhaften Systems

Bedrohung	Der Bund hat den Einsatz eines Systems bewilligt, das die bundesrechtlichen Sicherheitsanforderungen nicht erfüllt.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals d. Schutz der persönlichen Informationen über die stimmberechtigten Personen e. Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
Auswirkungen	
Evaluation	

	Ersteinschätzung
Wahrscheinlichkeit	Mittel

Anschliessend wird beschrieben, was bei einem Eintreten der Bedrohung passieren würde. Hier wird vom worst-case-Szenario ausgegangen, das in Textform beschrieben wird, um die Auswirkungen aufzuzeigen.

Risiko_1 Zulassung eines mangelhaften Systems

Bedrohung	Der Bund hat den Einsatz eines Systems bewilligt, das die bundesrechtlichen Sicherheitsanforderungen nicht erfüllt.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals d. Schutz der persönlichen Informationen über die stimmberechtigten Personen e. Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
Auswirkungen	Wenn ein Missbrauch des Systems nicht ausgeschlossen werden kann und die Stimmbeteiligung über den elektronischen Stimmkanal so gross war, dass dadurch das gesamte Ergebnis des Urnengangs verändert werden könnte, muss der Urnengang mit grosser Wahrscheinlichkeit für ungültig erklärt werden. Das Ansehen der Behörden wird schwer geschädigt und die Versuche mit der elektronischen Stimmabgabe müssen eingestellt werden.
Evaluation	

	Ersteinschätzung
Wahrscheinlichkeit	Mittel

Diese qualitative Analyse (Auswirkungen) muss nun in eine quantitative Analyse überführt werden. Diese Umwandlung kann nicht nur anhand einer mathematischen Formel erfolgen. Es gilt, auch Fachkompetenz und Erfahrung einfliessen zu lassen, indem die in Kapitel 3.2 aufgeführte Tabelle mit den Kriterien zur Risikomessung sowie die darin enthaltene Gewichtung angewendet werden. Die quantitative Analyse ergibt einen Risiko-Score, anhand dessen eine Priorisierung der Risikobehandlung vorgenommen wird.

Wirkungs-bereich	Kriterien zur Risikomessung				Score
	Tief (1)	**Mittel (2)**	**Hoch (3)**	**Gewicht**	
Reputation und Vertrauen	Die Glaubwürdigkeit der Bundesbehörden ist nicht oder nur geringfügig beeinträchtigt.	Die Glaubwürdigkeit der Bundesbehörden ist mittelschwer beeinträchtigt.	Die Glaubwürdigkeit der Bundesbehörden ist schwer beeinträchtigt.	5	3 x 5 = 15
	Die Korrektheit der Ergebnisse der Urnengänge wird nicht in Frage gestellt.	Die Korrektheit der Ergebnisse der Urnengänge wird geringfügig in Frage gestellt.	Die Korrektheit der Ergebnisse der Urnengänge wird weitgehend in Frage gestellt.		
Rechtliches	Der Bundesrat kann die Ergebnisse der Urnengänge ohne Verzögerung erwahren.	Der Bundesrat kann die Ergebnisse der Urnengänge mit Verzögerung erwahren.	Der Bundesrat kann die Ergebnisse der Urnengänge nicht erwahren.	5	3 x 5 = 15
	Die Integrität des Urnengangs ist intakt.	Es fand eine isolierte Manipulation von Stimmen statt.	Es fand eine systematische Manipulation von Stimmen statt.		
	Das Stimmgeheimnis wurde nicht verletzt.	Das Stimmgeheimnis wurde vereinzelt verletzt.	Das Stimmgeheimnis wurde systematisch verletzt.		
Kontinuität des elektronischen Stimmkanals	Der weitere Einsatz von E-Voting wird nicht oder nur geringfügig in Frage gestellt.	Der weitere Einsatz von E-Voting wird ernsthaft in Frage gestellt.	E-Voting muss mit hoher Wahrscheinlichkeit eingestellt werden.	3	3 x 3 = 9
Finanzen	Die wiederkehrenden Kosten für das Projekt Vote électronique der BK steigen nicht an.	Die wiederkehrenden Kosten für das Projekt Vote électronique der BK steigen moderat an.	Die wiederkehrenden Kosten für das Projekt Vote électronique der BK steigen signifikant an.	3	2 x 3 = 6
	Es gibt keinen oder nur einen moderaten einmaligen Kostenanstieg.	Es gibt einen signifikanten einmaligen Kostenanstieg.			
Produktivität	Der Arbeitsaufwand nimmt nicht oder nur punktuell und mässig zu.	Der Arbeitsaufwand nimmt entweder dauerhaft, aber nur mässig, oder punktuell, aber deutlich zu.	Der Arbeitsaufwand nimmt dauerhaft und deutlich zu.	1	2 x 1 = 2
Total Score					**47**

Nach Abschluss der Analyse- und Evaluationsphase wird das Risiko wie folgt beschrieben:

Risiko_1	***Zulassung eines mangelhaften Systems***
Bedrohung	Der Bund hat den Einsatz eines Systems bewilligt, das die bundesrechtlichen Sicherheitsanforderungen nicht erfüllt.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals d. Schutz der persönlichen Informationen über die stimmberechtigten Personen e. Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
Auswirkungen	Wenn ein Missbrauch des Systems nicht ausgeschlossen werden kann und die Stimmbeteiligung über den elektronischen Stimmkanal so gross war, dass dadurch das gesamte Ergebnis des Urnengangs verändert werden könnte, muss der Urnengang mit grosser Wahrscheinlichkeit für ungültig erklärt werden. Das Ansehen der Behörden wird schwer geschädigt und die Versuche mit der elektronischen Stimmabgabe müssen eingestellt werden.
Evaluation	

	Ersteinschätzung	
Wahrscheinlichkeit	Mittel	
Kriterien	**Wert**	**Score**
Reputation und Vertrauen	Hoch (3)	15
Rechtliches	Hoch (3)	15
Kontinuität	Hoch (3)	9
Finanzen	Mittel (2)	6
Produktivität	Mittel (2)	2
Risiko-Score		**47**

5.3 Risikobehandlung (Umgang)

Der Risiko-Score und die Eintretenswahrscheinlichkeit des Risikos bestimmen die Handlungsmöglichkeiten gemäss der Strategie zum Umgang mit Risiken, wie sie in Kapitel 3.3 definiert wird. Im vorliegenden Beispiel haben wir ein Risiko mit einer Wahrscheinlichkeit «mittel» und einem Risiko-Score von 47:

Wahrscheinlichkeit	**Score**		
	32 – 49	**22 – 31**	**17 – 21**
Hoch	Minimieren	Minimieren	Minimieren Beobachten
Mittel	Minimieren	Minimieren Beobachten	Minimieren Beobachten Akzeptieren
Tief	Minimieren Beobachten	Minimieren Beobachten Akzeptieren	Minimieren Beobachten Akzeptieren

Es ist daher nicht möglich, eine andere Massnahme als die Risikominimierung zu wählen. Nun müssen die Bedingungen für die Risikominimierung festgelegt werden. Diese können so gewählt werden, dass sie entweder die Eintretenswahrscheinlichkeit der Bedrohung verringern und / oder dass die Auswirkungen eines Eintretens der Bedrohung minimiert werden.

ID	Umgang	Massnahmen

Risiko_1	Minimieren	- Rechtliche Anforderungen:
		  - Limitierung des kantonalen Elektorats auf 30 % und des gesamtschweizerischen Elektorats auf 10 % (Art. 27*f* VPR)
		  - Überprüfung der Systeme und der Betriebsmodalitäten (Art. 27*l* VPR und Art. 10 VEleS)
		  - Offenlegung des Quellcodes und der Dokumentation zum System und dessen Betrieb (Art. 11 und 12 VEleS)
		  - Einbezug der Öffentlichkeit (Art. 13 VEleS)
		  - Feststellung und Meldung von Sicherheitsereignissen und -schwächen; Handhabung von Sicherheitsereignissen und -verbesserungen (Ziff. 14 Anhang VEleS)
		  - Entwicklung und Wartung von Informationssystemen (Ziff. 24 Anhang VEleS)
		  - Qualität Quellcode und Dokumentation (Ziff. 25 Anhang VEleS)
		- Führen eines gemeinsamen Massnahmenplans von Bund und Kantonen

Im vorliegenden Beispielfall haben insbesondere die Massnahmen zur Limitierung des Elektorats und zur Erkennung, Meldung und Behandlung von Vorfällen und Sicherheitsmängeln einen Einfluss auf die Folgen einer solchen Bedrohung und können deren Auswirkungen minimieren. Die Massnahmen zur unabhängigen sowie öffentlichen Überprüfung hingegen wirken insbesondere auf die Eintretenswahrscheinlichkeit der Bedrohung ein und verringern diese weiter.

5.4 Restrisiken

Nachdem die Massnahmen zur Risikobehandlung ergriffen wurden, muss das Risiko neu evaluiert werden. Damit wird geprüft, ob das Risiko auf ein akzeptierbares Niveau verringert werden konnte. Die erneute Evaluation erfolgt auf dieselbe Weise wie die erste Evaluation und wird in der Tabelle mit der Ersteinschätzung ergänzt.

Risiko_1 Zulassung eines mangelhaften Systems

Bedrohung	Der Bund hat den Einsatz eines Systems bewilligt, das die bundesrechtlichen Sicherheitsanforderungen nicht erfüllt.
Sicherheitsziele *(Art. 4 Abs. 3 VEleS)*	a. Korrektheit des Ergebnisses b. Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen c. Erreichbarkeit und Funktionsfähigkeit des Stimmkanals d. Schutz der persönlichen Informationen über die stimmberechtigten Personen e. Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen f. keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
Auswirkungen	Wenn ein Missbrauch des Systems nicht ausgeschlossen werden kann und die Stimmbeteiligung über den elektronischen Stimmkanal so gross war, dass dadurch das gesamte Ergebnis des Urnengangs verändert werden könnte, muss der Urnengang mit grosser Wahrscheinlichkeit für ungültig erklärt werden. Das Ansehen der Behörden wird schwer geschädigt und die Versuche mit der elektronischen Stimmabgabe müssen eingestellt werden.
Evaluation	

	Ersteinschätzung		**Nach der Minimierung**	
Wahrscheinlichkeit	Mittel		Tief	
Kriterien	**Wert**	**Score**	**Wert**	**Score**
Reputation und Vertrauen	Hoch (3)	15	Mittel (2)	10
Rechtliches	Hoch (3)	15	Mittel (2)	10
Kontinuität	Hoch (3)	9	Tief (1)	3
Finanzen	Mittel (2)	6	Tief (1)	3
Produktivität	Mittel (2)	2	Tief (1)	1
Risiko-Score		**47**		**27**

Mit einer Wahrscheinlichkeit «tief» und einem Risiko-Score von 27 ist das Risiko nun auf einem Niveau, das akzeptiert werden kann.

Wahrscheinlichkeit	**Score**		
	32 – 49	**22 – 31**	**17 – 21**
Hoch	Minimieren	Minimieren	Minimieren Beobachten
Mittel	Minimieren	Minimieren Beobachten	Minimieren Beobachten Akzeptieren
Tief	Minimieren Beobachten	Minimieren Beobachten Akzeptieren	Minimieren Beobachten Akzeptieren