Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizerische Bundeskanzlei BK

Sektion Politische Rechte

04. Oktober 2022

Leitfaden für Risikobeurteilungen

E-Voting-System der Schweizerischen Post

Dossiernummer: 431.0-2/5/13/1/2

1 Glossar

Informationsressourcen	Besonders wichtige Datenelemente, deren Integrität, Vertraulichkeit und/oder Verfügbarkeit geschützt werden müssen. Informationsressourcen können in materieller Form vorliegen (z.B. Computer, Server, Drucker) oder als Software (z.B. Verifier), als Information (z.B. Prüfcodes), als Teil einer Infrastruktur (z.B. Räume in Gebäuden), als Personen (z.B. Mitglieder des Wahlbüros oder als Dienst (z.B. Verwaltungsportal). Dieser Begriff wurde direkt aus der «OCTAVE Allegro»-Methodologie abgeleitet.
Hilfsmittel für die stimmberechtigten Personen	Die Gesamtheit der Informationen, die es den stimmberechtigten Personen erlauben, den Stimmvorgang in Einklang mit den Sicherheitsmassnahmen durchzuführen. Dazu gehören beispielsweise das Vorgehen zur Verifizierung der Ziffernfolge des Zertifikats des Wahl- oder Abstimmungsportals oder das Vorgehen zur Verifizierung verschiedener Codes.
Backend	Abstimmungs- oder Wahl-Server, der die elektronische Urne und Kontrollkomponenten enthält.
Wahlbüro	Personen, die nach kantonalem Recht für den ordnungsgemässen Ablauf des Urnengangs verantwortlich sind; im Rahmen der elektronischen Stimmabgabe sind dies Personen, welche die Urnen ver- und entschlüsseln.
Smartcards der Administratoren	Zertifikate, mit denen sich eine Person beim SDM authentifizieren kann.
Smartcards der Mitglieder des Wahlbüros	Smartcards, von denen jede einen Teil der Verschlüsselung einer elektronischen Urne enthält.
Stimmrechtsausweis	Ein Dokument, das es den stimmberechtigten Personen erlaubt, ihr Stimmrecht wahrzunehmen.
Signaturzertifikate	Zertifikate zur Authentifizierung der Kommunikation zwischen bestimmten Elementen des Systems.
Zertifikat des Wahl- oder Abstimmungsportals	Öffentlicher Schlüssel des Wahl- oder Abstimmungsportals, das für die Verschlüsselung der elektronisch abgegebenen Stimmen verwendet wird.
Initialisierungscode auf dem Stimmrechtsausweis	Der Initialisierungscode ergänzt die Daten zur Identifizierung der stimmberechtigten Personen; er ist auf dem Stimmrechtsausweis aufgedruckt und erlaubt es den stimmberechtigten Personen, ihre Stimme abzugeben.
Verifizierungscodes für die Stimmabgabe	Die auf dem Stimmrechtsausweis aufgedruckten Prüfcodes, Bestätigungscode und Finalisierungscode.
D0	Vorbereitung des Urnengangs.
D1	Tag, an dem die elektronischen Urnen konfiguriert, diese an das Online-System der Schweizerischen Post übermittelt und die Stimmrechtsausweise generiert werden.
D2	Tag, an dem die elektronischen Urnen durch das Wahlbüro verschlüsselt werden (einschliesslich der Generierung des Schlüssels des Wahlbüros).
D3	Tag, an dem die elektronischen Urnen mit dem Schlüssel des Wahlbüros entschlüsselt und die Ergebnisse der elektronischen Stimmabgabe ermittelt werden.
D4	Tag, an dem alle auf PC, Datenträger (z.B. USB-Sticks) und Smartcards gespeicherten Daten eines Urnengangs vernichtet werden. Ab diesem Tag sind die PC bereit für einen neuen Urnengang.

DIS (Data Integration Service)	Software der Schweizerischen Post zur Generierung der Konfigurationsdateien eines Urnengangs, die in der Informatik-Infrastruktur der Kantone installiert ist und dort betrieben wird: • Daten der stimmberechtigten Personen: zur Generierung des Stimmrechtsausweises via den dafür genutzten Dienst; • Daten des Urnengangs: für den Import in das Administrationsportal.
Daten zur Identifizierung der stimmberechtigten Personen	Datenelemente zur Identifizierung der stimmberechtigten Personen, die nicht auf dem Stimmrechtsausweis enthalten sind (z.B. Geburtsdatum oder -jahr, Identifizierung an einem virtuellen Schalter).
Journale und Histories (Logs)	Gesamtheit der Daten, mit denen das korrekte Funktionieren des Stimmvorgangs festgestellt werden kann oder anhand deren eine allfällige Fehlfunktion untersucht werden kann. Logs können in digitaler Form oder in Papierform vorliegen.
Software der Einwohnerdienste	Software zur Generierung der Datei oder der Dateien eCH-0045, die eine Liste der stimmberechtigten Personen enthält.
Vorbereitungssoftware	Software zur Generierung der Dateien eCH-0157 und/oder eCH-0159, welche die Parameter des Urnengangs und/oder den Gegenstand des Urnengangs enthalten (z.B. kantonales Ergebnisermittlungssystem).
Passwörter der Administratoren	Passwörter zur Entschlüsselung des auf der entsprechenden Smartcard gespeicherten Zertifikats.
Passwörter der Mitglieder des Wahlbüros	Passwörter zur Entschlüsselung des jeweiligen Teils des Schlüssels, der auf der entsprechenden Smartcard gespeichert ist.
Gegenstand des Urnengangs	Abstimmungsfragen, die den stimmberechtigten Personen bei Abstimmungen unterbreitet werden, bzw. Listen mit den Kandidatinnen und Kandidaten bei Wahlen. Diese befinden sich insbesondere in den Dateien mit dem Format eCH-0159 respektive eCH-0157.
Parameter des Urnengangs	Basisdaten des Urnengangs, beispielsweise das Datum des Urnengangs, die Daten und die Zeiten, zu denen die Stimmabgabe möglich ist, die Art der Abstimmung und/oder Wahl, die Sicherheitsparameter (z.B. die Anzahl der Mitglieder des Wahlbüros).
Administrationsportal	Web-Portal der Schweizerischen Post, das von den kantonalen Administratorinnen und Administratoren zur elektronischen Stimmabgabe verwendet wird.
Wahl- oder Abstimmungsportal	Web-Portal der Schweizerischen Post, das von den stimmenden Personen genutzt wird.
EV-Stimmregister	Register der stimmberechtigten Personen, die zur elektronischen Stimmabgabe zugelassen sind. Dieses Register befindet sich insbesondere in der Datei mit dem Format eCH-0045.
EV-Ergebnisse	Ergebnisse der Auszählung der elektronischen Urne. Die Ergebnisse befinden sich insbesondere in Dateien mit dem Format eCH-0110 und eCH-0222.
SDM (Secure Data Manager)	Software der Schweizerischen Post, die in der Informatik-Infrastruktur der Kantone installiert ist und dort betrieben wird. Die Software ist auf mehrere, voneinander getrennte Computer verteilt, die mit keinem Netzwerk verbunden sind; die Software läuft ferner auf einem PC, der mit der Infrastruktur der Schweizerischen Post verbunden ist. Sie ermöglicht die folgenden Arbeiten: • Verwaltung der kryptografischen Informationen, mit denen die Integrität und die Sicherheit des Stimmvorgangs überwacht werden können; • Generierung der Identifizierungsdaten auf dem Stimmrechtsausweis;

	• Generierung der Verifizierungscodes; • Verschlüsselung der elektronischen Urnen mithilfe des Schlüssels des Wahlbüros; • Entschlüsselung der abgegebenen Stimmen unter Wahrung des Stimmgeheimnisses.
Software zur Generierung der Stimmrechtsausweise	Software, die für die Generierung der Stimmrechtsausweise im Format PostScript und/oder PDF verwendet wird.
Elektronische Stimmen	Stimmen, deren Inhalt der Eingabe der stimmenden Person auf dem Wahl- oder Abstimmungsportal entspricht.
Verifier	Ein vom Wahlbüro verwendetes technisches Hilfsmittel, mit dem die vom Backend stammenden Beweise, dass die Ergebnisse korrekt festgestellt worden sind, geprüft werden. Die Schweizerische Post bietet eine Open-Source-Software, die auf einem separaten Offline-Laptop installiert und vom Kanton betrieben wird.
Briefliche Stimmabgabe, Stimmabgabe an der Urne	Gesamtheit der Stimm- und Wahlzettel, die per brieflicher Stimmabgabe (dazu gehört auch die Hinterlegung im Stimmlokal der Wohngemeinde) oder durch Stimmabgabe an der Urne im Stimmlokal abgegeben worden sind.

2 Thematische Verortung und Ziel des Leitfadens

Bei der Ausübung der politischen Rechte besteht eine föderalistische Kompetenzaufteilung. Für eidgenössische Urnengänge werden auf Bundesebene die Rahmenbedingungen festgelegt und die Kantone sind für die Durchführung zuständig. Diese Kompetenzaufteilung gilt auch im Bereich der elektronischen Stimmabgabe und ist in den bestehenden Rechtsgrundlagen zu den Versuchen mit E-Voting abgebildet. Demnach entscheiden die Kantone, ob sie ihren stimmberechtigten Personen die elektronische Stimmabgabe im Rahmen eines Versuchs zur Verfügung stellen wollen. Sie können dafür ein eigenes System betreiben oder das System eines anderen Kantons oder eines privaten Unternehmens nutzen (Art. 27*k*^{bis} Abs. 1 Bst. b Verordnung über die politischen Rechte, VPR). Der Bund ist für die Bewilligung und Zulassung der Versuche zuständig, unterstützt die Kantone in rechtlichen, organisatorischen und technischen Belangen und koordiniert die Vorhaben auf nationaler Ebene. Der Bund ist bei der elektronischen Stimmabgabe stark involviert (Art. 8*a* Abs. 4 des Bundesgesetzes über die politischen Rechte, BPR). Er legt – mit grossem Detaillierungsgrad – in der Verordnung der BK vom 25. Mai 2022 über die elektronische Stimmabgabe (VEleS) die technischen und organisatorischen Anforderungen fest.

Der Kanton ist für die Durchführung von eidgenössischen Urnengängen verantwortlich und trägt die Risiken beim Einsatz der elektronischen Stimmabgabe. Er muss mit einer Risikobeurteilung darlegen, dass sich jegliche Sicherheitsrisiken in einem ausreichend tiefen Rahmen bewegen. Die Anforderungen an die Risikobeurteilungen sind in Artikel 4 in Verbindung mit Artikel 9 VEleS festgehalten.

Das vorliegende Dokument ist ein Leitfaden für die Erstellung von Risikobeurteilungen durch die Bundeskanzlei, die Kantone und die Schweizerische Post als Systemanbieterin. Darin wird das grundlegende Vorgehen zur Erstellung von Risikobeurteilungen beschrieben und die Zuständigkeiten festgelegt. Ziel des Leitfadens ist es, die Vollständigkeit und Relevanz von Risikobeurteilungen zu gewährleisten, den Akteuren den Vorgang der Risikobeurteilung zugänglicher zu machen und die Verantwortlichkeiten auf diesem Gebiet zu definieren.

Dieser Leitfaden wurde gemeinsam von der Bundeskanzlei, den Kantonen und der Schweizerischen Post (nachstehend Post genannt) erarbeitet. Er muss regelmässig auf seine Aktualität hin überprüft und gegebenenfalls angepasst werden. Der Leitfaden geht auf die, in den rechtlichen Grundlagen definierten Anforderungen ein und überträgt sie auf den konkreten Fall des E-Voting-Systems der Post. Sollte dereinst ein anderes E-Voting-System verwendet werden, so muss ein spezifisch auf dieses System zugeschnittener Leitfaden erarbeitet werden.

3 Zu behandelnde Sicherheitsziele

Artikel 4 VEleS umreisst die Ziele und die Leitlinien der Risikobeurteilung. Insbesondere werden in Absatz 3 die verschiedenen Sicherheitsziele, die zu beachten sind, festgelegt.

4 Methodologie der Risikobeurteilung

Der vorliegende Leitfaden wurde auf Grundlage der «OCTAVE Allegro»-Methodik[1] verfasst. Er basiert also auf dem Grundkonzept von «OCTAVE Allegro», ist aber dennoch so allgemein verfasst, dass er auch für jegliche anderen methodischen Ansätze verwendet werden kann, solange sie die folgenden Tätigkeiten umfassen:

(1) Erarbeitung einer Risikomanagementrichtlinie

(2) Identifizierung von Kernprozessen

(3) Identifizierung von Informationsressourcen, die im Zusammenhang mit Kernprozessen stehen, und Definition des Schutzes, der für diese Ressourcen notwendig ist

(4) Identifizierung technischer und physischer Elemente sowie der Personen, von denen die Informationsressourcen abhängen

(5) Identifizierung von Bedrohungsszenarien für jede Informationsressource

(6) Risikoidentifizierung

(7) Risikoanalyse

(8) Risikoevaluation

(9) Umgang mit Risiken

4.1 Erarbeitung einer Risikomanagementrichtlinie

Die Risikomanagementrichtlinie ist grundlegend für die Risikobeurteilung. Sie definiert den Prozess der Risikoevaluation, einschliesslich dessen Periodizität, der Evaluationskriterien, der Methode zur Messung der Risikoauswirkungen und die Regeln zum Umgang mit Risiken. Damit die Risikomanagementrichtlinie angemessen bleibt, muss sie regelmässig einer Überprüfung unterzogen werden.

4.2 Identifizierung von Kernprozessen

Für jede Phase eines Urnengangs müssen die verschiedenen Kernprozesse identifiziert werden. Mit diesen können die zu schützenden Informationsressourcen identifiziert werden.

Grundsätzlich und auch im Fall des E-Voting-Systems der Post gliedert sich ein Urnengang in folgende Phasen:

- Vorbereitung
  - Vorbereitung der Dateien für die elektronische Stimmabgabe (Gegenstand des Urnengangs und Stimmregister) (D0)
  - Vorbereitung der Parameter des Urnengangs (D1)
  - Vorbereitung der elektronischen Urne (D1)
  - Generierung der Schlüssel zur Verschlüsselung für die Administratoren des Urnengangs (D1)
  - Generierung der Codes (ID der stimmberechtigten Personen, Initialisierung, Verifizierung, Bestätigung, Finalisierung) (D1)
  - Generierung der Stimmrechtsausweise (D1)
  - Druck der Stimmrechtsausweise (D1)
  - Versand der Abstimmungsunterlagen (D1)

[1] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process

- Initialisierung
  - Initialisierung der elektronischen Urne (D2)
  - Generierung der Schlüssel zur Verschlüsselung für die Mitglieder des Wahlbüros (D2)
  - Versiegelung der elektronischen Urne (D2)
  - Verifizierung vor dem Urnengang (D2)
  - Bereitstellung der Urne im VoterPortal der Post (D2)
  - Von den Administratoren durchgeführte Teststimmabgabe (inklusive Auszählung) (D2)
  - Durch das Wahlbüro durchgeführte Kontrollstimmabgabe (D2)
  - Sicherung von Geräten und Hilfsmitteln (D2)

- Stimmabgabe
  - Öffnung des elektronischen Stimmkanals
  - Kontrolle der Stimmrechtsausweise (elektronische Stimmabgabe, briefliche Stimmabgabe, Stimmabgabe im Abstimmungslokal)
  - Schliessung des elektronischen Stimmkanals

- Abschluss
  - Mixing (Online): Entfernung nicht bestätigte Stimmen (Cleansing) und erstes Mischen der Stimmen (D3)
  - Herunterladen der Urne(n) (D3)
  - Verifizierung (VerifyOnlineTally) (D3)
  - Mixing und Entschlüsseln der gültigen Stimmen (Offline) (D3)
  - Verifizierung (VerifyOfflineTally) (D3)
  - Kontrolle der Kontrollstimmen des Wahlbüros (D3)
  - Zusammenführen der Resultate aus den verschiedenen Stimmkanälen (D3)
  - Sicherung von Geräten und Hilfsmitteln (D3)

- Nach dem Urnengang
  - Löschen der Dateien (D4)
  - Sicheres Löschen/Formatieren oder Vernichtung der Datenträger (D4)
  - Vernichtung der gespeicherten Passwörter (D4)
  - Vernichtung der Smartcards (D4)

4.3 Identifizierung von Informationsressourcen, die im Zusammenhang mit Kernprozessen stehen, und Definition des Schutzes, der für diese Ressourcen notwendig ist

Die Umsetzung der oben erwähnten Sicherheitsziele setzt voraus, dass die Informationsressourcen sowohl innerhalb als auch ausserhalb der Infrastruktur identifiziert werden. Die Identifizierung basiert auf der Analyse von Kernprozessen, die im vorangehenden Unterkapitel definiert wurden.

Für die folgenden Informationsressourcen sind die folgenden Stellen zuständig:

Informations-ressourcen	**Zuständigkeit in Abhängigkeit von der Phase des Urnengangs**				
	Vorbereitung	**Initialisierung**	**Stimmabgabe**	**Abschluss**	**Nach dem Urnengang**
Parameter des Urnengangs	Kanton	Kanton Post	Post		
EV-Stimmregister	Kanton	Kanton			
Gegenstand des Urnengangs	Kanton	Kanton Post Druckerei	Post		
Hilfsmittel für die stimmberechtigten Personen		Kanton Druckerei	Kanton Post		
Smartcards der Administratoren	Kanton	Kanton	Kanton	Kanton	Kanton

Informations-ressourcen	Zuständigkeit in Abhängigkeit von der Phase des Urnengangs				
	Vorbereitung	**Initialisierung**	**Stimmabgabe**	**Abschluss**	**Nach dem Urnengang**
Passwörter der Administratoren	Kanton	Kanton	Kanton	Kanton	Kanton
Daten zur Identifizierung der stimmberechtigten Personen		Kanton Post	Kanton Post		
Initialisierungscode auf dem Stimmrechtsausweis	Kanton	Kanton Post Druckerei	Kanton Post		
Verifizierungscodes für die Stimmabgabe	Kanton	Kanton Post Druckerei	Kanton Poste		
Smartcards der Mitglieder des Wahlbüros		Kanton	Kanton	Kanton	Kanton
Passwörter der Mitglieder des Wahlbüros		Kanton	Kanton	Kanton	Kanton
Software der Einwohnerdienste	Kanton				
Vorbereitungssoftware	Kanton				
DIS		Kanton			
SDM		Kanton		Kanton	
Dienst zur Generierung des Stimmrechtsausweises		Kanton			
Administrationsportal		Kanton Post		Kanton Post	Post
Wahl- oder Abstimmungsportal		Post	Post		
Backend		Post	Post	Post	Post
Verifier		Kanton		Kanton	
Zertifikat des Wahl- oder Abstimmungsportals	Post	Post	Post	Post	Post
Elektronische Stimmen		Kanton Post	Post stimmberechtigte Personen	Kanton Post	Kanton Post
Briefliche Stimmabgabe, Stimmabgabe an der Urne			Kanton stimmberechtigte Personen	Kanton	Kanton
EV-Ergebnisse				Kanton	Kanton
Journale und Histories (Logs)	Kanton	Kanton Post	Kanton Post	Kanton Post	Kanton Post
Signaturzertifikate	Kanton	Kanton Post		Kanton Post	

Diese Tabelle hat einen allgemeinen Charakter; sie kann von den Kantonen nach ihren jeweiligen Bedürfnissen vervollständigt werden. Die identifizierten Informationsressourcen können zusammengefasst oder aber im Rahmen der Risikobeurteilung sofern sinnvoll in mehrere Einheiten unterteilt werden. In diesem Fall muss eine Verbindung zwischen den hier erwähnten Informationsressourcen und den gebildeten Gruppen hergestellt werden.

Für jede Informationsressource muss eine verantwortliche Person definiert werden. Diese definiert dann die Schutzanforderungen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit. Die Schutzanforderungen gewisser Informationsressourcen können von anderen Ressourcen abhängen; es empfiehlt sich deshalb, dies zu berücksichtigen, wenn die Schutzanforderungen dieser anderen Informationsressourcen definiert werden.

4.4 Identifizierung technischer und physischer Elemente sowie der Personen, von denen die Informationsressourcen abhängen

Identifizierte Informationsressourcen können durch unterschiedliche Mittel (in der «OCTAVE Allegro»-Methodik «Container» genannt) bearbeitet, gespeichert oder übermittelt werden. Die Mittel können einen grossen Einfluss auf die Erfüllung der Schutzanforderungen von Informationsressourcen haben. Deshalb ist es notwendig, für jede Informationsressource die erwähnten Mittel oder Container aufzulisten.

Eine erste Gruppe von Containern wird durch das technische Umfeld einer Informationsressource gebildet: Es besteht einerseits aus Geräten (Computern der Benutzerinnen und Benutzer und Servern) sowie aus Software, mit welcher die Informationsressource bearbeitet, gespeichert oder übermittelt wird, andererseits aus Verbindungen (Kabel, Netzwerke, USB-Sticks, etc.), die der Übermittlung der Informationsressource dienen. Besonderes Augenmerk muss hier auf die Teilnehmerinnen und Teilnehmer des Systems und auf sichere Kommunikationskanäle (z.B. Kontrollkomponenten, technisches Hilfsmittel der Prüferinnen und Prüfer (Verifier), Setup-Komponente, Druckkomponente) gelegt werden. Die technischen Container können anhand der folgenden Fragen identifiziert werden:

- Welche Informationssysteme (Software) verwenden oder bearbeiten die fragliche Informationsressource?
- Auf welche Weise wird diese Informationsressource von einem Informationssystem zum anderen übermittelt?
- Auf welchem Informatikmaterial (Hardware) befindet sich die fragliche Informationsressource?

Eine zweite Gruppe von Containern wird durch das physische Umfeld der Informationsressource gebildet. Dazu gehören Tresore und andere gesicherte Orte, in denen Informationsressourcen aufbewahrt werden; eine Informationsressource selbst kann aber auch in physischer Form vorliegen, beispielsweise auf Papier. Die physischen Container können anhand der folgenden Frage identifiziert werden:

- Gibt es Papierkopien der fraglichen Informationsressource?
- Gibt es Orte zur physischen Aufbewahrung der fraglichen Informationsressource?

Eine letzte Gruppe von Containern wird durch Personen im Umfeld der Informationsressource gebildet. Dieses Umfeld umfasst verschiedene Personen, welche die Informationsressource kennen. Dieser Aspekt ist wichtig bei Passwörtern oder bei jedem Element, das geheim gehalten werden muss oder dessen Integrität von grösster Wichtigkeit ist. Die personellen Container können anhand der folgenden Fragen identifiziert werden:

- Welche Personen (stimmberechtigte Personen, Administratorinnen und Administratoren, Personal, Prüferinnen und Prüfer, etc.) könnten Zugang zur fraglichen Informationsressource haben und könnten sich diese merken oder sie weitergeben?

4.5 Identifizierung von Bedrohungsszenarien für jede Informationsressource

In einem zweiten Schritt werden alle im vorherigen Schritt ermittelten technischen, physischen und personellen Elemente geprüft. Dabei wird festgestellt, welche Ereignisse die Schutzanforderungen der einzelnen Informationsressourcen gefährden könnten. Diese Ereignisse können durch interne oder externe

Personen willentlich oder unabsichtlich verursacht werden, oder es kann sich um eine Fehlfunktion handeln. Für eine systematische Analyse kann es sinnvoll sein, die Bedrohungen mit einem Ereignisbaum abzubilden. Auf dieser Grundlage können Bedrohungsszenarien identifiziert werden. Dabei müssen nur Bedrohungen der oben genannten Sicherheitsziele erfasst werden. Die unter Ziffer 13 des Anhangs der VEleS beschriebenen Bedrohungen (vgl. die untenstehende Tabelle) müssen dabei ebenso berücksichtigt werden wie Szenarien, die sich dadurch ergeben, dass die Stimmabgabe über verschiedene Kanäle möglich ist.

Referenz	Beschreibung	Betroffene Sicherheitsziele	Informationsressource
13.3	Malware verändert die Stimme auf der Benutzerplattform.	Korrektheit des Ergebnisses	Elektronische Stimmen
13.4	Ein externer Angreifer leitet die Stimme mittels Domain-Name-Server-Spoofing (DNS-Spoofing) um.	Korrektheit des Ergebnisses	Elektronische Stimmen
13.5	Ein externer Angreifer verändert die Stimme mit einer Man-in-the-middle-Technik (MITM -Technik).	Korrektheit des Ergebnisses	Elektronische Stimmen
13.6	Ein externer Angreifer schickt mittels MITM bösartig veränderte Daten, die für die Stimmabgabe notwendig sind und aus dem Online-System stammen (z. B. Javascript-Datei).	Korrektheit des Ergebnisses	Wahl- oder Abstimmungsportal
13.7	Ein interner Angreifer manipuliert die Software, diese speichert die Stimmen nicht.	Korrektheit des Ergebnisses	Backend
13.8	Ein interner Angreifer verändert, löscht oder vervielfacht die Stimmen.	Korrektheit des Ergebnisses	Elektronische Stimmen
13.9	Ein interner Angreifer fügt Stimmen ein.	Korrektheit des Ergebnisses	Backend
13.10	Eine feindliche Organisation dringt in das System ein mit dem Ziel, das Ergebnis zu fälschen.	Korrektheit des Ergebnisses	Backend
13.11	Ein interner Angreifer kopiert Stimmunterlagen und benutzt sie.	Korrektheit des Ergebnisses	Initialisierungscode auf dem Stimmrechtsausweis Verifizierungscodes für die Stimmabgabe
13.12	Ein externer Angreifer nutzt Social-Engineering-Methoden, um die Aufmerksamkeit der stimmenden Person an den Sicherheitsvorkehrungen vorbeizulenken (individuelle Verifizierbarkeit).	Korrektheit des Ergebnisses	Hilfsmittel für die stimmberechtigten Personen
13.13	Ein externer Angreifer dringt elektronisch, physisch oder mittels Social Engineering in die Infrastruktur des Kantons ein und manipuliert die Setup-Komponente oder entwendet sicherheitsrelevante Daten.	Korrektheit des Ergebnisses	Parameter des Urnengangs SDM
13.14	Ein externer Angreifer dringt elektronisch, physisch oder mittels Social Engineering in die Infrastruktur der Druckerei ein und entnimmt die Codes der Stimmrechtsausweise.	Korrektheit des Ergebnisses	Initialisierungscode auf dem Stimmrechtsausweis Verifizierungscodes für die Stimmabgabe

Referenz	Beschreibung	Betroffene Sicherheitsziele	Informationsressource
13.15	Ein externer Angreifer dringt elektronisch, physisch oder mittels Social Engineering in die Infrastruktur der Post ein und entwendet Stimmrechtsausweise.	Korrektheit des Ergebnisses	Initialisierungscode auf dem Stimmrechtsausweis Verifizierungscodes für die Stimmabgabe
13.16	In der individuellen Verifizierbarkeit tritt ein Fehler auf.	Korrektheit des Ergebnisses	Backend
13.17	In der universellen Verifizierbarkeit tritt ein Fehler auf.	Korrektheit des Ergebnisses	Backend
13.18	Ein technisches Hilfsmittel der Prüferinnen und Prüfer weist einen Fehler auf.	Korrektheit des Ergebnisses	Verifier
13.19	Eine Backdoor wird über eine Softwareabhängigkeit in das System eingeführt und von einem externen Angreifer ausgenutzt, um auf das System zuzugreifen.	Korrektheit des Ergebnisses, Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen, Erreichbarkeit und Funktionsfähigkeit des Stimmkanals, Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen, keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten	Wahl- oder Abstimmungsportal Backend
13.20	Malware auf der Benutzerplattform schickt die Stimme an eine feindliche Organisation.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	Elektronische Stimmen
13.21	Die Stimme wird mittels DNS-Spoofing umgeleitet.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	Elektronische Stimmen
13.22	Ein externer Angreifer liest die Stimme mittels MITM.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	Elektronische Stimmen
13.23	Ein interner Angreifer benutzt den Schlüssel und entschlüsselt nicht-anonyme Stimmen.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	Smartcards der Mitglieder des Wahlbüros Passwörter der Mitglieder des Wahlbüros Elektronische Stimmen
13.24	Bei der Prüfung auf Korrektheit der Verarbeitung und der Auszählung wird das Stimmgeheimnis gebrochen.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	SDM Verifier Elektronische Stimmen
13.25	Ein interner Angreifer liest die Stimmen vorzeitig, ohne die Stimmen entschlüsseln zu müssen.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	Backend
13.26	Eine feindliche Organisation dringt ins System ein mit dem Ziel, das Stimmgeheimnis zu brechen oder Teilergebnisse vorzeitig zu erheben.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	Backend

Referenz	Beschreibung	Betroffene Sicherheitsziele	Informationsressource
13.27	Ein Fehler im Verschlüsselungsprozess macht diesen funktionsunfähig oder reduziert seine Wirksamkeit.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	Backend Elektronische Stimmen
13.28	Ein interner Angreifer manipuliert die Software und diese legt die Stimmen offen.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	Backend
13.29	Malware auf der Benutzerplattform macht die Stimmabgabe unmöglich.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Hilfsmittel für die stimmberechtigten Personen
13.30	Eine feindliche Organisation führt einen Denial-of-Service-Angriff (DOS-Angriff) durch.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Administrationsportal Wahl- oder Abstimmungsportal
13.31	Ein interner Angreifer nimmt eine fehlerhafte Konfiguration vor; es kommt nicht bis zur Auszählung.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	EV-Ergebnisse
13.32	Ein interner Angreifer fälscht die kryptografischen Beweise der universellen Verifizierbarkeit.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Journale und Histories (Logs)
13.33	Ein technischer Fehler des Systems führt dazu, dass das System zum Zeitpunkt der Auszählung nicht verfügbar ist.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Administrationsportal Backend
13.34	Ein technisches Hilfsmittel der Prüferinnen und Prüfer funktioniert zum Zeitpunkt der Auszählung nicht.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Verifier
13.35	Eine feindliche Organisation dringt ins System ein mit dem Ziel, den Betrieb zu stören, die Informationen für die stimmberechtigten Personen zu manipulieren oder Beweise zum Stimmverhalten der stimmenden Personen zu stehlen.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals, Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen, keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten	Gegenstand des Urnengangs Hilfsmittel für die stimmberechtigten Personen Wahl- oder Abstimmungsportal Backend
13.36	Ein interner Angreifer stiehlt Adressdaten der stimmberechtigten Personen.	Schutz der persönlichen Informationen über die Stimmberechtigen	EV-Stimmregister Software der Einwohnerdienste DIS SDM Dienst zur Generierung des Stimmrechtsausweises
13.37	Malware beeinflusst stimmberechtigte Personen bei der Meinungsbildung.	Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen	Gegenstand des Urnengangs Hilfsmittel für die stimmberechtigten Personen
13.38	Ein interner Angreifer manipuliert die Informationswebsite bzw. das Abstimmungsportal und täuscht so die stimmberechtigten Personen.	Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen	Gegenstand des Urnengangs Hilfsmittel für die stimmberechtigten Personen Wahl- oder Abstimmungsportal

Referenz	Beschreibung	Betroffene Sicherheitsziele	Informationsressource
13.39	Ein interner Angreifer schreibt stimmberechtigten Personen vor, ob und wie sie abzustimmen oder zu wählen haben. Nach der Entschlüsselung findet er in der Infrastruktur Belege, dass sich die stimmberechtigten Personen an die Instruktionen gehalten haben.	Keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten	Backend
13.40	Ein externer Angreifer schreibt stimmberechtigten Personen vor, ob und wie sie abzustimmen oder zu wählen haben und verlangt von ihnen einen Beleg, dass sie sich an die Instruktionen gehalten haben.	Keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten	Elektronische Stimmen

4.6 Risikoidentifizierung

Ein Risiko liegt dann vor, wenn die Möglichkeit eines Schadens oder eines Verlusts besteht. Dieses bezieht sich auf eine Situation, in der eine Person etwas Unerwünschtes tun oder ein Ereignis ein unerwünschtes Ergebnis zur Folge haben könnte, was sich negativ auf die Erreichung der Sicherheitsziele auswirken könnte. Ein Risiko besteht aus:

- einem Ereignis, das durch einen Akteur, ein Mittel (z.B. die Ausnutzung eines Fehlers oder mehrerer Fehler) und eine betroffene Informationsressource bestimmt ist
- einer Auswirkung
- einer Ungewissheit

Bei der Risikoidentifizierung geht es darum, die im vorhergehenden Kapitel identifizierten Bedrohungsszenarien unter dem Blickwinkel der Risiken zu dokumentieren. Insbesondere soll ermittelt werden, welche Auswirkungen das Eintreten eines jeden Bedrohungsszenarios haben könnte. Idealerweise müssten alle Auswirkungen dokumentiert werden, aber es ist zulässig, für jedes der Risiken nur die gravierendste Auswirkung aufzuzeigen.

Da der Kanton die Hauptverantwortung für den geordneten Ablauf eines Urnengangs hat, muss er bei der Risikobeurteilung alle mit dem Urnengang zusammenhängenden Risiken identifizieren.

Der Systemanbieter ist gegenüber dem Kanton für den geordneten Betrieb des Systems verantwortlich. Die Identifizierung der Risiken durch den Systemanbieter muss auf den durch den Kanton identifizierten Risiken basieren und in Abhängigkeit von den verwendeten technischen und organisatorischen Mitteln erweitert werden. Auch hier ist es angezeigt, ein systematisches Vorgehen und eine für die verwendeten Mittel angemessene Detailtiefe zu wählen. Ereignisbäume können hierzu ein wertvolles Hilfsmittel sein.

Grundsätzlich sollten alle Risiken, die in einer vorgängigen Risikobeurteilung enthalten waren, bei einer weiteren Risikobeurteilung nochmals beleuchtet werden. Risiken, die immer noch relevant sind, müssen in der neuen Risikobeurteilung übernommen und aktualisiert werden.

Beispiel:

Bedrohungsszenario	Risiko	Auswirkung
Ein externer Angreifer dringt elektronisch, physisch oder mittels Social Engineering in die Infrastruktur der Druckerei ein und entnimmt die Codes der Stimmrechtsausweise.	Ein Aktivist in einem Bereich, für welchen der Ausgang eines Urnengangs einen Einfluss haben kann, gibt sich als Druckmaschinenmechaniker aus und nutzt den Zugang zur Druckereiinfrastruktur, um eine Kamera zu installieren, dank der er die Initialisierungscodes der Stimmrechtsausweise sieht.	Die Kamera bleibt unentdeckt, und der Angreifer hat eine grosse Zahl von Initialisierungscodes gespeichert. Er findet in sozialen Netzwerken einen Teil der passenden Geburtsdaten und benutzt sie, um Stimmen abzugeben. Einige stimmberechtigte Personen sind erstaunt, dass sie ihr Stimmmaterial nicht verwenden können und kontaktieren die Staatskanzlei. Diese schliesst den elektronischen Stimmkanal und leitet eine Ermittlung ein. Medien werden auf die Affäre aufmerksam und berichten in grossem Stil darüber, was der Staatskanzlei einen grossen Kommunikationsaufwand beschert. Beschwerden werden eingereicht, und dies führt zur Aufhebung des Urnengangs.

4.7 Risikoanalyse

Die Risikoanalyse ist eine komplexe Angelegenheit. Im Rahmen einer strukturierten Evaluation der Risiken ist es angezeigt, die Auswirkungen, die ein Risiko haben kann, systematisch zu analysieren.

Zunächst muss die Bedeutung der Auswirkungen der im vorhergehenden Unterkapitel identifizierten Risiken anhand der in der Risikomanagementrichtlinie definierten Evaluationskriterien qualitativ eingeschätzt werden. Konkret geht es darum, die Beschreibung der Auswirkungen eines jeden Risikos anhand der vorgängig definierten Evaluationskriterien in eine numerische Form zu bringen. Für jedes Risiko müssen alle Kriterien evaluiert werden. Ferner muss die Evaluation anhand der Wichtigkeit des Kriteriums gewichtet werden.

Beispiel:

Unter Berücksichtigung der folgenden Evaluationskriterien:

Rang	Kriterien	Gering (1)	Mittel (2)	Hoch (3)
4	Reputation und Vertrauen	Die Reputation hat nur geringfügig gelitten; sie kann mit geringem oder sogar ohne Aufwand wiederhergestellt werden.	Die Reputation hat substanziell gelitten; um sie wiederherzustellen, sind Anstrengungen nötig.	Die Reputation hat unwiederbringlich Schaden erlitten.
3	Finanzen	Die jährlichen Betriebskosten erhöhen sich um weniger als 10%.	Die jährlichen Betriebskosten erhöhen sich zwischen 10% und 20%.	Die jährlichen Betriebskosten erhöhen sich um mehr als 20%.
2	Rechtliches	Das Beschwerderisiko ist im Vergleich zu anderen Abstimmungskanälen nicht signifikant höher.	Das Beschwerderisiko ist im Vergleich zu anderen Abstimmungskanälen signifikant höher.	Dass eine Beschwerde erhoben wird, ist sozusagen sicher.
1	Produktivität	Die Arbeitslast der Bereiche Politische Rechte und Informatik einer Staatskanzlei erhöht sich um weniger als 20%.	Die Arbeitslast der Bereiche Politische Rechte und Informatik einer Staatskanzlei erhöht sich zwischen 20% und 50%.	Die Arbeitslast der Bereiche Politische Rechte und Informatik einer Staatskanzlei erhöht sich um mehr als 50%.

Die Risikoanalyse ergibt:

Risiko	Auswirkung	Kriterien	Score
Ein Aktivist in einem Bereich, für welchen der Ausgang des Urnengangs einen Einfluss haben kann, gibt sich als Druckmaschinenmechaniker aus und nutzt den Zugang zur Druckereiinfrastruktur, um eine Kamera zu installieren, dank der er die Initialisierungscodes des Stimmrechtsausweises sieht.	Die Kamera bleibt unentdeckt, und der Angreifer hat eine grosse Zahl von Initialisierungscodes gespeichert. Er findet in sozialen Netzwerken einen Teil der passenden Geburtsdaten und benutzt sie, um Stimmen abzugeben. Einige stimmberechtigte Personen sind erstaunt, dass sie ihr Stimmmaterial nicht verwenden können und kontaktieren die Staatskanzlei. Diese schliesst den elektronischen Stimmkanal und leitet eine Ermittlung ein. Medien werden auf die Affäre aufmerksam und berichten in grossem Stil darüber, was der Staatskanzlei einen grossen Kommunikationsaufwand beschert. Beschwerden werden eingereicht, und dies führt zur Aufhebung des Urnengangs.	Reputation und Vertrauen	2 (Mittel) x 4 (Rang) = 8
		Finanzen	2 (Mittel) x 3 (Rang) = 6
		Rechtliches	3 (Hoch) x 2 (Rang) = 6
		Produktivität	1 (Gering) x 1 (Rang) = 1
		Total	8 + 6 + 6 + 1 = 21

Zusätzlich zum so errechneten Risiko-Score kann es angezeigt sein, die Eintrittswahrscheinlichkeit eines Risikos einzubeziehen. Für die Bestimmung der Eintrittswahrscheinlichkeit wird eine Zeitspanne von drei Jahren (oder ungefähr zehn eidgenössische Urnengänge) berücksichtigt. Die Beurteilungen werden dann nach der folgenden Abstufung vorgenommen:

- Hoch: Sehr wahrscheinliches Szenario: Es ist sehr wahrscheinlich, dass ein solches Ereignis innerhalb von zehn Urnengängen eintritt (Wahrscheinlichkeit höher als 30%).
- Mittel: 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%).
- Gering: Unwahrscheinliches Szenario: Innerhalb von zehn Urnengängen tritt kein solches Ereignis ein (Wahrscheinlichkeit weniger als 3%).

Wenn die Eintrittswahrscheinlichkeit einbezogen wird, muss sie aufgrund des systematischen Vorgehens für alle und nicht nur für ausgewählte Risiken definiert werden.

4.8 Risikoevaluation

Der in der vorhergehenden Etappe errechnete Risiko-Score – der allenfalls noch mit der Eintrittswahrscheinlichkeit kombiniert wird – muss nun mit der Risikomanagementrichtlinie verbunden werden. Dies erlaubt es, die Risiken untereinander zu priorisieren und diejenigen Risiken zu identifizieren, die ein Handeln erfordern.

4.9 Umgang mit Risiken

Die Risikomanagementrichtlinie definiert den Umgang mit Risiken nach deren Wichtigkeit. Grundsätzlich kann ein Risiko:

- akzeptiert werden: Dies erfordert kein Handeln.
- überwacht werden: Messgrössen werden definiert und regelmässig überwacht.
- minimiert werden: Eine oder mehrere Massnahmen werden ergriffen, mit denen die Auswirkungen oder die Eintrittswahrscheinlichkeit eines Risikos reduziert werden sollen.

- abgewälzt werden: Risiken werden mittels einer Versicherung oder durch entsprechende Vertragsklauseln auf Dritte abgewälzt.

Der Kanton ist zwar für alle Risiken im Zusammenhang mit einem Urnengang verantwortlich; er kann aber einen Teil davon mittels Vertrag auf Dritte abwälzen. Dieser Vertrag wird dann eine eigene Massnahme zur Risikominimierung, die durch Kontrollmassnahmen (Visiten, regelmässige schriftliche Berichte, etc.) ergänzt werden kann. Das Restrisiko besteht dann darin, dass der beauftragte Dritte entweder seinen Pflichten nicht nachgekommen ist, nicht wirksame Massnahmen ergriffen oder das Risiko in Kauf genommen hat.

Möglicherweise kann ein Risiko nicht wirksam minimiert werden, obwohl dies gemäss der Risikomanagementrichtlinie erforderlich wäre. In diesem Fall muss die Ausnahme von der kantonalen Stelle, die im Sinne der VEleS zuständig ist, begründet und ausdrücklich gutgeheissen werden.

Die Anforderungen gemäss Anhang der VEleS stellen eine nicht abschliessende Liste von Massnahmen zur Risikominimierung dar. Die wichtigsten dieser Massnahmen werden in der nachfolgenden Tabelle dargestellt:

Referenz	Beschreibung	Betroffene Sicherheitsziele	Anforderungen gemäss Anhang der VEleS
13.3	Malware verändert die Stimme auf der Benutzerplattform.	Korrektheit des Ergebnisses	2.5, 2.12, 4.3, 8.4, 8.5, 8.8, 8.11
13.4	Ein externer Angreifer leitet die Stimme mittels Domain-Name-Server-Spoofing (DNS-Spoofing) um.	Korrektheit des Ergebnisses	2.5, 4.3, 8.4, 8.5, 8.8, 8.10, 8.11
13.5	Ein externer Angreifer verändert die Stimme mit einer Man-in-the-middle-Technik (MITM - Technik).	Korrektheit des Ergebnisses	2.5, 2.12, 4.3, 8.4, 8.5, 8.8, 8.11, 15.2
13.6	Ein externer Angreifer schickt mittels MITM bösartig veränderte Daten, die für die Stimmabgabe notwendig sind und aus dem Online-System stammen (z. B. Javascript-Datei).	Korrektheit des Ergebnisses	8.10, 10, 15.2
13.7	Ein interner Angreifer manipuliert die Software, diese speichert die Stimmen nicht.	Korrektheit des Ergebnisses	3.6, 3.7, 3.14, 14.1, 22.1, 22.3, 24.1, 24.3
13.8	Ein interner Angreifer verändert, löscht oder vervielfacht die Stimmen.	Korrektheit des Ergebnisses	2.6, 3.3, 3.14, 3.16, 5.2, 14.7, 22.1, 22.3
13.9	Ein interner Angreifer fügt Stimmen ein.	Korrektheit des Ergebnisses	2.6, 3.3, 3.14, 3.16, 5.2, 14.7, 22.1, 22.3
13.10	Eine feindliche Organisation dringt in das System ein mit dem Ziel, das Ergebnis zu fälschen.	Korrektheit des Ergebnisses	2.6, 3.3, 3.14, 3.16, 5.2, 14.1, 14.7, 15.2, 16.1, 16.2
13.11	Ein interner Angreifer kopiert Stimmunterlagen und benutzt sie.	Korrektheit des Ergebnisses	2.8, 3.10, 3.14, 4.9, 6.2, 6.3, 7.1, 22.1, 22.3, 22.5

Referenz	Beschreibung	Betroffene Sicherheitsziele	Anforderungen gemäss Anhang der VEleS
13.12	Ein externer Angreifer nutzt Social-Engineering-Methoden, um die Aufmerksamkeit der stimmenden Person an den Sicherheitsvorkehrungen vorbeizulenken (individuelle Verifizierbarkeit).	Korrektheit des Ergebnisses	4.3, 8.3, 8.4, 8.11
13.13	Ein externer Angreifer dringt elektronisch, physisch oder mittels Social Engineering in die Infrastruktur des Kantons ein und manipuliert die Setup-Komponente oder entwendet sicherheitsrelevante Daten.	Korrektheit des Ergebnisses	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	Ein externer Angreifer dringt elektronisch, physisch oder mittels Social Engineering in die Infrastruktur der Druckerei ein und entnimmt die Codes der Stimmrechtsausweise.	Korrektheit des Ergebnisses	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	Ein externer Angreifer dringt elektronisch, physisch oder mittels Social Engineering in die Infrastruktur der Post ein und entwendet Stimmrechtsausweise.	Korrektheit des Ergebnisses	3.8, 7.8, 18.3, 21.2, 21.3, 23.5
13.16	In der individuellen Verifizierbarkeit tritt ein Fehler auf.	Korrektheit des Ergebnisses	17.1, 17.2, 17.3, 24.4, 25.13
13.17	In der universellen Verifizierbarkeit tritt ein Fehler auf.	Korrektheit des Ergebnisses	17.1, 17.2, 17.3, 24.4, 25.13
13.18	Ein technisches Hilfsmittel der Prüferinnen und Prüfer weist einen Fehler auf.	Korrektheit des Ergebnisses	17.1, 17.2, 17.3, 24.4, 25.13
13.19	Eine Backdoor wird über eine Softwareabhängigkeit in das System eingeführt und von einem externen Angreifer ausgenutzt, um auf das System zuzugreifen.	Korrektheit des Ergebnisses, Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen, Erreichbarkeit und Funktionsfähigkeit des Stimmkanals, Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen, keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten	3.8, 3.15, 3.16, 3.18, 14.1, 16.1, 16.2, 22.2, 22.4, 24.3
13.20	Malware auf der Benutzerplattform schickt die Stimme an eine feindliche Organisation.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	8.5, 8.6, 15.2
13.21	Die Stimme wird mittels DNS-Spoofing umgeleitet.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	2.7, 8.10, 8.11
13.22	Ein externer Angreifer liest die Stimme mittels MITM.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	2.7, 8.10, 8.11, 15.2

Referenz	Beschreibung	Betroffene Sicherheitsziele	Anforderungen gemäss Anhang der VEIeS
13.23	Ein interner Angreifer benutzt den Schlüssel und entschlüsselt nicht-anonyme Stimmen.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	3.1, 3.10, 3.14, 12.1, 12.2, 12.3, 22.1, 22.3
13.24	Bei der Prüfung auf Korrektheit der Verarbeitung und der Auszählung wird das Stimmgeheimnis gebrochen.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	2.7, 3.10, 3.13, 3.14, 8.14, 12.1
13.25	Ein interner Angreifer liest die Stimmen vorzeitig, ohne die Stimmen entschlüsseln zu müssen.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	2.7, 3.2, 3.8, 3.14, 12.2, 15.2, 15.3, 22.1, 22.3
13.26	Eine feindliche Organisation dringt ins System ein mit dem Ziel, das Stimmgeheimnis zu brechen oder Teilergebnisse vorzeitig zu erheben.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	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	Ein Fehler im Verschlüsselungsprozess macht diesen funktionsunfähig oder reduziert seine Wirksamkeit.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	3.8, 15.4, 16.1, 24.4
13.28	Ein interner Angreifer manipuliert die Software und diese legt die Stimmen offen.	Wahrung des Stimmgeheimnisses und Ausschluss von vorzeitigen Teilergebnissen	3.6, 3.7, 3.11, 3.15, 12.2, 24.3
13.29	Malware auf der Benutzerplattform macht die Stimmabgabe unmöglich.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	4.3, 8.1, 8.2, 8.3, 8.5, 8.8, 8.11
13.30	Eine feindliche Organisation führt einen Denial-of-Service-Angriff (DOS-Angriff) durch.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	14.1, 14.8
13.31	Ein interner Angreifer nimmt eine fehlerhafte Konfiguration vor; es kommt nicht bis zur Auszählung.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	3.6, 3.8, 3.10, 24.2
13.32	Ein interner Angreifer fälscht die kryptografischen Beweise der universellen Verifizierbarkeit.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	2.11, 3.8, 3.14, 3.16, 14.1, 22.1, 22.3
13.33	Ein technischer Fehler des Systems führt dazu, dass das System zum Zeitpunkt der Auszählung nicht verfügbar ist.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	14.1, 25.8, 25.13
13.34	Ein technisches Hilfsmittel der Prüferinnen und Prüfer funktioniert zum Zeitpunkt der Auszählung nicht.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	25.8, 25.13
13.35	Eine feindliche Organisation dringt ins System ein mit dem Ziel, den Betrieb zu stören, die Informationen für die stimmberechtigten Personen zu manipulieren oder Beweise zum Stimmverhalten der stimmenden Personen zu stehlen.	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals, Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen, keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten	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

Referenz	Beschreibung	Betroffene Sicherheitsziele	Anforderungen gemäss Anhang der VEleS
13.36	Ein interner Angreifer stiehlt Adressdaten der stimmberechtigten Personen.	Schutz der persönlichen Informationen über die Stimmberechtigen	3.10, 3.14, 5.1, 21.3, 22.1, 22.3
13.37	Malware beeinflusst stimmberechtigte Personen bei der Meinungsbildung.	Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen	8.3, 8.5, 8.10, 8.11
13.38	Ein interner Angreifer manipuliert die Informationswebsite bzw. das Abstimmungsportal und täuscht so die stimmberechtigten Personen.	Schutz der für die stimmberechtigten Personen bestimmten Informationen vor Manipulationen	4.3, 8.2, 8.3, 8.5, 8.7, 8.10, 8.11, 14.1, 22.1, 22.3, 23.3
13.39	Ein interner Angreifer schreibt stimmberechtigten Personen vor, ob und wie sie abzustimmen oder zu wählen haben. Nach der Entschlüsselung findet er in der Infrastruktur Belege, dass sich die stimmberechtigten Personen an die Instruktionen gehalten haben.	Keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten	3.10, 3.14, 11.4, 11.7, 12.1, 12.5, 15.2, 15.3, 22.1, 22.3
13.40	Ein externer Angreifer schreibt stimmberechtigten Personen vor, ob und wie sie abzustimmen oder zu wählen haben und verlangt von ihnen einen Beleg, dass sie sich an die Instruktionen gehalten haben.	Keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten	4.7, 4.8

Die in den rechtlichen Bestimmungen vorgesehenen Massnahmen reichen gegebenenfalls nicht aus. Sie müssen mit zusätzlichen Massnahmen ergänzt werden, bis die Risiken hinreichend gering sind (Art. 9 VEleS).

Trotz aller ergriffenen Massnahmen zur Risikominimierung kann das Risiko nicht auf null reduziert werden – sei es, weil die ergriffene Massnahme nicht zu 100 Prozent wirksam ist, oder weil sie nur einen Teil des Risikos zu minimieren vermag. In diesem Fall muss das Restrisiko eindeutig identifiziert werden und den im Rahmen der Risikomanagementrichtlinie festgelegten Akzeptanzkriterien entsprechen.

5 Mit den Bereichen Politik und Verwaltung zusammenhängende Risiken

Nebst den Risiken, die sich beim Betrieb eines E-Voting-Systems ergeben, müssen auch die Risiken aus den Bereichen Politik und Verwaltung beurteilt werden, d.h. aus Bereichen, die keinen direkten Zusammenhang mit dem Betrieb des Systems haben. Diese Risiken betreffen die kantonale Ebene und in gewissen Fällen auch die Ebene des Bundes. In der folgenden Tabelle werden die mindestens zu berücksichtigenden Risiken dargestellt:

Risiko		Bereich
RPA-1	Gegen einen Kanton wird Beschwerde eingereicht, weil er ein System betrieben und dabei ungenügende Sicherheitsmassnahmen ergriffen hat.	Rechtliches
RPA-2	Der Bund hat ein System zugelassen, das die bundesrechtlichen Sicherheitsanforderungen nicht erfüllt.	Rechtliches
RPA-3	Streitigkeiten zwischen den Behörden und der Post stören die Zusammenarbeit derart stark, dass der elektronische Stimmkanal nicht mehr weiterentwickelt werden kann oder unterbrochen werden muss.	Finanzen

RPA-4	Die Untersuchung eines Angriffs auf den elektronischen Stimmkanal kann wegen fehlender technischer Möglichkeiten nicht ordentlich durchgeführt werden.	Reputation und Vertrauen
RPA-5	Ein Angriff auf den elektronischen Stimmkanal kann wegen fehlender rechtlicher Möglichkeiten nicht verfolgt werden.	Reputation und Vertrauen
RPA-6	In den Medien oder in sozialen Netzwerken wird eine Kampagne gegen den elektronischen Stimmkanal geführt. Diese kann auf Ereignissen rund um die elektronische Stimmabgabe im Ausland, auf angeblich fehlenden öffentlichen Kontrollmöglichkeiten, auf falschen Behauptungen über die Mechanismen der Verifizierbarkeit oder auf einer mangelhaften Kommunikation der Behörden beruhen.	Reputation und Vertrauen
RPA-7	Bei der Auszählung stellt sich heraus, dass die Ergebnisse der elektronischen Stimmabgabe von den Ergebnissen der anderen Stimmkanäle abweichen.	Reputation und Vertrauen
RPA-8	Den Kantonen fehlen die Ressourcen für die Umsetzung des elektronischen Stimmkanals.	Finanzen
RPA-9	Eine Gruppe, die über eine anonyme Kaufplattform verfügt, lanciert eine grossangelegte Kampagne zum Stimmenkauf.	Reputation und Vertrauen
RPA-10	Während der Phase der Stimmabgabe ereignet sich ein sicherheitsrelevanter Vorfall und es wird nicht innert nützlicher Frist adäquat reagiert.	Reputation und Vertrauen

6 Rolle der Bundeskanzlei bei der Risikobeurteilung

Die BK erarbeitet für das Projekt «Vote électronique» ihre eigene Risikobeurteilung. Dafür beurteilt sie sowohl die allgemeinen technischen Risiken als auch die Risiken im Zusammenhang mit den Bereichen Politik und Verwaltung. Die Situation der Kantone und der Post fliesst ebenfalls in diese Beurteilung ein. Die Risikobeurteilung der BK wird den Kantonen zugestellt, die sie bei der Erarbeitung ihrer eigenen Risikobeurteilung verwenden können. Sie wird zudem auf der Internetseite der BK veröffentlicht.

Die Bundeskanzlei steht den Kantonen bei Fragen zur Risikobeurteilung gerne zur Verfügung.