# Richtlinie Risikomanagement

E-Voting Basel-Stadt / Graubünden / St.Gallen / Thurgau

| | |
|---|---|
| Autoren | **Projektleitung E-Voting (BS)**<br>**E-Voting Beauftragter (GR)**<br>**Leitung der elektronischen Stimmabgabe (SG)**<br>**Fachperson E-Voting (TG)** |
| Datum | 29.09.2023 |
| Version | 1.2 |
| Klassifizierung | Keine |

## Änderungskontrolle

| Version | Datum | Beschreibung | Name |
|---|---|---|---|
| 1.0 | 21.12.2022 | Freigegebene Version | Projektleitung E-Voting (BS)<br>Leitung Informatik und Infrastruktur (SG)<br>Fachperson E-Voting (TG) |
| 1.1 | 28.04.2023 | Integration von Graubünden<br>Neuer Abschnitt (2.1) | Projektleitung E-Voting (BS)<br>E-Voting Beauftragter (GR)<br>Leitung Informatik und Infrastruktur (SG)<br>Fachperson E-Voting (TG) |
| 1.2 | 29.09.2023 | Formelle Anpassungen | Projektleitung E-Voting (BS)<br>E-Voting Beauftragter (GR)<br>Leitung Informatik und Infrastruktur (SG)<br>Fachperson E-Voting (TG) |

## Prüf-/Freigabestellen

| Prüfer | Freigeber | Datum |
|---|---|---|
| Leitung Recht und Volksrechte (BS)<br>Leitung Dienst für politische Rechte (SG)<br>Leitung Rechtsdienst (TG) | Leitung Staatskanzlei (BS)<br>Leitung Staatskanzlei (SG)<br>Leitung Staatskanzlei (TG) | 12.12.2022 |
| Leitung Abteilung Services (GR) | Leitung Standeskanzlei (GR) | 22.09.2023 |

## Referenzierte Dokumente

| Nr. | Dokument | Version |
|---|---|---|
| [1] | Verordnung der BK über die elektronische Stimmabgabe (VEleS, SR 161.116) vom 25. Mai 2022 | Stand am 1. Juli 2022 |
| [2] | "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process" des Software Engineering Institutes (SEI)<br>https://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419 | Version 1.0 vom Mai 2007 |
| [3] | Leitfaden für Risikobeurteilungen der Schweizerischen Bundeskanzlei für das E-Voting-System der Schweizerischen Post<br>https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Vote--lectronique/Leitfaden%20BK_Risikobeurteilungen%20Vote%20%C3%A9lectronique,%20Oktober%202022.pdf.download.pdf/Leitfaden%20BK_Risikobeurteilungen%20Vote%20%C3%A9lectronique,%20Oktober%202022.pdf | Version vom 04.10.2022 |
| [4] | Richtlinie Informationssicherheit | Aktuelle Version |
| [5] | Glossar | Aktuelle Version |

# Inhaltsverzeichnis

# 1 Zweck des Dokuments

Das vorliegende Dokument behandelt die Methodik für die Beurteilung und den Umgang mit Risiken im Rahmen der elektronischen Stimmabgabe.

# 2 Einleitung

Die Richtlinie bildet die Grundlage 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.

Die Richtlinie wird einer regelmässigen Überprüfung unterzogen, um die Aktualität zu gewährleisten.

## 2.1 Massnahmen gemäss der VEleS

Als Ausgangslage der Risikobeurteilung werden die Massnahmen gemäss der Verordnung der BK über die elektronische Stimmabgabe (VEleS) als umgesetzt betrachtet. Bei allfälligen Nichtkonformitäten wird die Risikobeurteilung mit den entsprechenden Risiken ergänzt.

Der Leitfaden der Bundeskanzlei (siehe *referenziertes Dokument [3]*) listet die Massnahmen auf, die die Bedrohungen adressieren (Tabelle in *Abschnitt 4.9* des Leitfadens). Die Risikoanalyse der Kantone beinhaltet die vollständigen Referenzen zu den Bedrohungen, die im Leitfaden definiert sind, um die Nachvollziehbarkeit zwischen den Risiken des Kantons und den Massnahmen gemäss VEleS sicherzustellen. Dies ist relevant für den Fall, dass eine Massnahme nicht wirken würde.

# 3 Sicherheitsziele

Die Risikobeurteilungen beziehen sich auf die folgenden Sicherheitsziele (gemäss Art. 4 der VEleS):

- Korrektheit des Ergebnisses
- Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
- Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
- Schutz der persönlichen Informationen über die Stimmberechtigten
- Schutz der für die Stimmberechtigten bestimmten Informationen vor Manipulationen
- Keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten

# 4 Prozess und Verantwortlichkeiten

Im Rahmen des Risikobeurteilungsprozesses wird ein Inventar der Informationsressourcen (inkl. Beschreibung in separaten Profilen gemäss *Abschnitt 5.2*) und ein Risikoportfolio (siehe *Abschnitt 5.3*) geführt. Verantwortlich für den Risikobeurteilungsprozess ist die Leitung der elektronischen Stimmabgabe. Sie fungiert als Risikoeigner für die im Risikoportfolio geführten Risiken. Der Risikoeigner ist dafür zuständig, die Risiken regelmässig gemäss Vorgabe zu prüfen und sicherzustellen, dass die Massnahmen rechtzeitig umgesetzt werden. Die Periodizität des Prozesses wird unter *Abschnitt 4.1* beschrieben.

Die jeweiligen Eigner der Informationsressourcen sind dafür zuständig, die Sicherheitsanforderungen der Informationsressourcen festzulegen und dafür zu sorgen, dass geeignete Schutzstrategien implementiert werden, um diese Anforderungen zu erfüllen.

## 4.1 Periodizität des Prozesses

Der Risikoeigner muss die bestehenden Risiken regelmässig überprüfen und das Risikoportfolio mit den allfällig neuen, identifizierten Risiken aktualisieren. Diese Überprüfung erfolgt mindestens einmal jährlich. Falls es zu wesentlichen organisatorischen, technologischen oder prozessualen Änderungen kommt, wird eine Überprüfung ausgelöst. Die Risiken, welche die Einstufung "zu überwachen" aufweisen, sind vor jedem Urnengang zu überprüfen (siehe *Abschnitt 9.3)*.

# 5 Methodik und Komponenten

## 5.1 Anwendung der Methode OCTAVE Allegro

Der Kanton orientiert sich an der Methode "OCTAVE Allegro" vom Software Engineering Institute (SEI) der Carnegie Mellon University (siehe *referenziertes Dokument [2]*), welche auch im Leitfaden der Bundeskanzlei (siehe *referenziertes Dokument [3]*) als Grundlage für die Risikobeurteilung herangezogen wurde.

Die Methode sieht die folgenden Schritte vor:

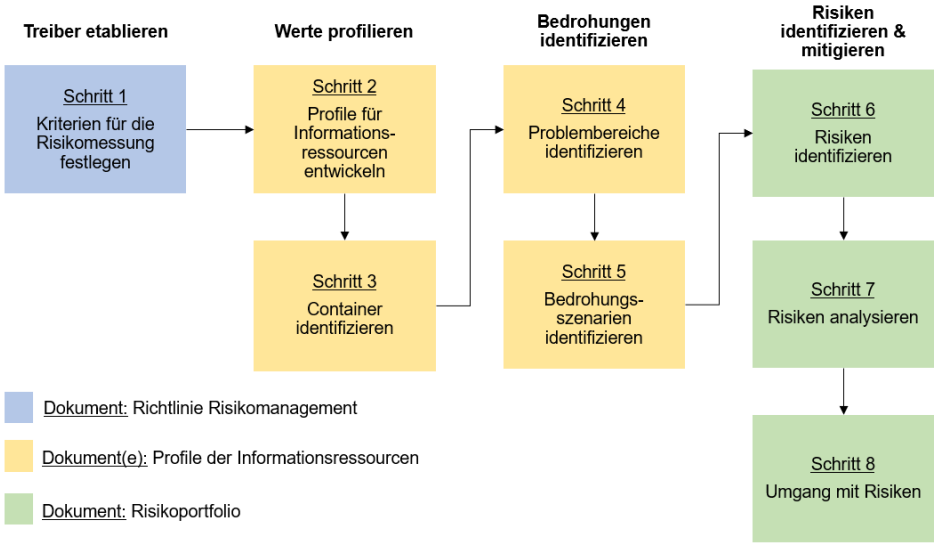


Abbildung 1: Schritte gemäss OCTAVE Allegro

Die Kriterien für die Risikomessung **(Schritt 1)** werden im vorliegenden Dokument definiert (siehe *Abschnitt 8).* Die Informationsressourcen und Container werden anhand der definierten Kernprozesse identifiziert.

Die Entwicklung der Profile für die Informationsressourcen **(Schritt 2)**, inklusive der dazugehörigen Container **(Schritt 3)** sowie die Identifikation der Problembereiche **(Schritt 4)** und Bedrohungsszenarien **(Schritt 5)**, erfolgt in den "Profilen der Informationsressourcen" (siehe *Abschnitt 5.2*).

Aus den Problembereichen und Bedrohungsszenarien der Profile ergeben sich die identifizierten Risiken **(Schritt 6)**. Die Risikoanalyse **(Schritt 7)** und die Risikobehandlung **(Schritt 8)** der identifizierten Risiken erfolgt im "Risikoportfolio" (siehe *Abschnitt 5.3*).

## 5.2 Profile der Informationsressourcen

Wie in *Abschnitt 5.1* erläutert, werden die **Schritte 2 bis 5** innerhalb der Profile der Informationsressourcen abgehandelt. Pro Profil wird eine Excel-Datei mit den nötigen Informationen gemäss Vorlage vom SEI (siehe *referenziertes Dokument [2]*) geführt. Die Profile enthalten jeweils die folgenden Inhalte:

- Beschreibung der Informationsressource
- Eigner der Informationsressource
- Beschreibung und Selektion der Sicherheitsanforderungen
- Auflistung und Beschreibung der Container
- Auflistung der Problembereiche und Bedrohungsszenarien (inkl. Mapping des Risikos)

Die vorgelagerte Identifizierung der Informationsressourcen wird in *Abschnitt 6* erläutert.

## 5.3 Risikoportfolio

Gemäss *Abschnitt 5.1* werden die **Schritte 6 bis 8** innerhalb des Risikoportfolios abgehandelt. Für die sich aus den Profilen ergebenden Bedrohungen werden die entsprechenden Risiken im Portfolio geführt, analysiert und behandelt. Pro Risiko wird ein separates Blatt mit den nötigen Informationen gemäss Vorlage vom SEI (siehe *referenziertes Dokument [2]*) als Teil des Portfolios geführt. Die Risiko-Blätter enthalten jeweils die folgenden Inhalte:

- Beschreibung der Bedrohung (Art und Wirkung des Risikos)
- Bewertung der Wahrscheinlichkeit des Eintretens
- Beschreibung und Bewertung der Auswirkung
- Resultierende Berechnung des Risiko-Scores und der Risikostufe
- Beschreibung und Selektion der Risikobehandlung

Die Beschreibung des jeweiligen Risikos wird ergänzt mit der Angabe der betroffenen Sicherheitsziele (siehe *Abschnitt 3*).

# 6 Identifizierung von Informationsressourcen und Container

Alle anhand der Kernprozesse identifizierten Informationsressourcen müssen analysiert werden. Es sind alle Informationsressourcen betroffen, welche die Vertraulichkeit, Integrität oder Verfügbarkeit der Informationen im Rahmen der elektronischen Stimmabgabe beeinträchtigen können.

Die Informationsressourcen können physische oder elektronische Dokumente, Applikationen und Datenbanken, Personen, IT-Einrichtungen, Infrastruktur und ausgelagerte Services/Prozesse umfassen. Bei der Identifikation der Informationsressourcen sind auch deren Eigner (die für jede Informationsressource verantwortlichen Personen oder Organisationseinheiten) sowie die Container zu identifizieren.

Die Container sind unterschiedliche Mittel, welche die Informationsressourcen bearbeiten, speichern oder übermitteln. Sie können in drei Gruppen unterteilt werden:

- Technisches Umfeld: Geräte (z.B. Computer), Software (z.B. IT-Applikation) oder Verbindungen (z.B. USB-Stick)
- Physisches Umfeld: Physisches Dokument, physisches Dossier, ein Raum, Tresor etc.
- Menschliches Umfeld: Person oder Gruppe, die Informationsressourcen kennen bzw. bearbeiten

Die identifizierten Informationsressourcen und Container werden im Inventar der Informationsressourcen geführt und in den Profilen der Informationsressourcen (siehe *Abschnitt 5.2)* analysiert.

Die Klassifizierung der Informationsressourcen gemäss dem Dokument "Richtlinie Informationssicherheit" (siehe *referenziertes Dokument [4]*) sowie die Zuordnung der identifizierten Informationsressourcen zu den Informationsressourcen aus dem Leitfaden der Bundeskanzlei (siehe *referenziertes Dokument [3]*) erfolgt im Inventar der Informationsressourcen.

# 7 Risikoidentifizierung

Auf der Grundlage der Informationsressourcen und den damit zusammenhängenden Containern wird festgestellt, welche Ereignisse die Schutzanforderungen der einzelnen Informationsressourcen gefährden könnten. Die Identifikation dieser möglichen Problembereiche und abgeleiteten Bedrohungsszenarien pro Informationsressource erfolgt über die Profile der Informationsressourcen (siehe *Abschnitt 5.2*) und bildet die Grundlage für die Risikoanalyse im Risikoportfolio (siehe *Abschnitt 5.3*).

# 8 Risikoanalyse: Kriterien zur Risikobeurteilung

Die Kriterien für die Risikomessung bilden die Grundlage der Risikobeurteilung und werden zu Beginn des Prozesses festgelegt. Der Risikoeigner und die Eigner der Informationsressourcen beurteilen anschliessend anhand der definierten Skala die Auswirkungen für jedes Risikoszenario sowie die Wahrscheinlichkeit eines Risikoeintritts.

Die Beurteilung erfolgt auf Grundlage der Vorgaben der Bundeskanzlei im Leitfaden (siehe *referenziertes Dokument [3]*). Die folgenden Abschnitte beschreiben die Evaluation der Kriterien und die darauf aufbauende Beurteilung.

## 8.1 Ermittlung der Auswirkung

Um die Auswirkungen zu definieren, werden die Risiken anhand Evaluationskriterien qualitativ eingeschätzt und in eine numerische Form gebracht.

Die folgenden Evaluationskriterien sind für die Analyse definiert:

- **Reputation und Vertrauen:** Auswirkung eines Risikos auf die Reputation oder das Vertrauen in Zusammenhang mit der elektronischen Stimmabgabe
- **Finanzen:** Finanzielle Auswirkung eines Risikos in Zusammenhang mit der elektronischen Stimmabgabe
- **Rechtliches:** Auswirkung eines Risikos auf die Konformität mit den gesetzlichen Vorgaben in Zusammenhang mit der elektronischen Stimmabgabe
- **Produktivität:** Auswirkung eines Risikos auf die betriebliche Produktivität

Für jedes Risiko müssen alle Kriterien evaluiert werden. Die Messung der Auswirkung erfolgt in zwei Schritten.

### 8.1.1 Schritt 1: Identifikation der Kritikalität

In einem ersten Schritt wird jedes Risiko anhand jedem Evaluationskriterium mit einer Einstufung der Kritikalität bewertet: **Tief, Mittel oder Hoch**

Die folgende Tabelle beschreibt anhand von ausgewählten Beispielen wie die Einstufung der Kritikalität für die einzelnen Kriterien ausgelegt ist.

| Wirkungsbereich | **Tief** | **Mittel** | **Hoch** |
|---|---|---|---|
| **Kriterium: Reputation und Vertrauen** | Die Reputation wird nur geringfügig beeinträchtigt; es müssen keine oder nur geringe Anstrengungen unternommen werden, um sie wiederherzustellen. | Die Reputation wird substanziell beeinträchtigt; es sind Anstrengungen nötig, um sie wiederherzustellen. | Die Reputation hat unwiederbringlich Schaden erlitten. |
| | Echo in den lokalen Medien. | Echo in den regionalen Medien. | Echo in den nationalen Medien. |
| **Kriterium: Finanzen** | Anstieg der jährlichen Betriebskosten um weniger als 10%. | Anstieg der jährlichen Betriebskosten um 10% bis 20%. | Anstieg der jährlichen Betriebskosten um mehr als 20%. |
| **Kriterium: Rechtliches** | Das Risiko einer erfolgreichen Beschwerde steigt nicht signifikant im Vergleich zu anderen Wahl- oder Abstimmungskanälen. | Das Risiko einer erfolgreichen Beschwerde steigt signifikant im Vergleich zu anderen Wahl- oder Abstimmungskanälen. | Eine erfolgreiche Beschwerde ist quasi sicher. |
| **Kriterium: Produktivität** | Erhöhung der Arbeitsbelastung der Bereiche politische Rechte und Informatik der Staatskanzlei / Standeskanzlei um weniger als 20%. | Erhöhung der Arbeitsbelastung der Bereiche politische Rechte und Informatik der Staatskanzlei / Standeskanzlei um 20% bis 50%. | Erhöhung der Arbeitsbelastung der Bereiche politische Rechte und Informatik der Staatskanzlei / Standeskanzlei um mehr als 50%. |

Tabelle 1: Beispiele Einstufung der Kritikalität der Evaluationskriterien

### 8.1.2 Schritt 2: Ermittlung des Risiko-Scores

In einem zweiten Schritt wird die Auswirkung der einzelnen Risiken durch die folgenden Formeln bestimmt:

- **Kriterium-Score** = Gewicht des Kriteriums multipliziert mit Gewicht der Kritikalität
- **Risiko-Score** = Summe der Kriterium-Scores

Die nachfolgende Tabelle zeigt auf, wie die Evaluationskriterien und die Kritikalität gewichtet werden.

| Gewichtung der Evaluationskriterien | |
|---|---|
| Reputation und Vertrauen | 4 |
| Finanzen | 3 |
| Rechtliches | 2 |
| Produktivität | 1 |
| **Gewichtung der Kritikalität** | |
| Hoch | 3 |
| Mittel | 2 |
| Tief | 1 |

Tabelle 2: Gewichtung von Kriterien und Kritikalität

## 8.2 Ermittlung der Wahrscheinlichkeit

Nach der Beurteilung der Auswirkung ist die Wahrscheinlichkeit des Eintretens für jedes Szenario zu beurteilen. Die Beurteilung der Wahrscheinlichkeit erfolgt anhand der folgenden Abstufungen:

- **Hoch (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%).

# 9 Risikobehandlung

## 9.1 Ermittlung der Risikostufe

Der in *Abschnitt 8.1* errechnete Risiko-Score wird mit der in *Abschnitt 8.2* definierten Eintrittswahrscheinlichkeit kombiniert, um die Risikostufe zu ermitteln (siehe *Tabelle 3*).

Die Risikostufe wird innerhalb des jeweiligen Risiko-Blatts im Risikoportfolio (siehe *Abschnitt 5.3*) anhand der getroffenen Auswahl automatisch berechnet.

Die Risikostufe erlaubt es, die Risiken im Rahmen der Risikobehandlung untereinander zu priorisieren und diejenigen Risiken zu identifizieren, die ein Handeln erfordern.

## 9.2 Risikoakzeptanzkriterien

Die nachfolgende Matrix beschreibt, wie die Risiken nach Risikostufe behandelt werden.

| | | | | |
|---|---|---|---|---|
| Auswirkung | **21-30** | Signifikantes Risiko: Zu überwachen | Untragbares Risiko: Zu minimieren | Untragbares Risiko: Zu minimieren |
| | **11-20** | Geringes Risiko: Akzeptiert | Signifikantes Risiko: Zu überwachen | Untragbares Risiko: Zu minimieren |
| | **10** | Geringes Risiko: Akzeptiert | Geringes Risiko: Akzeptiert | Signifikantes Risiko: Zu überwachen |
| | | **Gering** | **Mittel** | **Hoch** |
| | | Wahrscheinlichkeit | | |

Tabelle 3: Risikoakzeptanzkriterien

Der grundsätzliche Umgang mit den Risiken nach Risikostufe wird in *Abschnitt 9.3* beschrieben. Die Risikobehandlung kann jedoch aufgrund von fachlichen Entscheidungen auch abweichend definiert werden. So kann beispielsweise festgelegt werden, dass ein bestimmtes signifikantes Risiko nicht nur überwacht, sondern auch minimiert werden soll.

## 9.3 Umgang mit Risiken

Die Risikobehandlung wird mithilfe des Risikoportfolios (siehe *Abschnitt 5.3*) umgesetzt und durch die Leitung der elektronischen Stimmabgabe durchgeführt. Die möglichen Optionen für den Umgang mit Risiken werden in der nachfolgenden Tabelle erläutert.

| | |
|---|---|
| **Akzeptiert** | Dies erfordert kein Handeln. Es erfolgt jedoch eine regelmässige Überprüfung der Beurteilung (jährlich oder bei wesentlichen organisatorischen, technologischen oder prozessualen Änderungen). |
| **Zu überwachen** | Risiken werden regelmässig überwacht. Eine Überprüfung wird vor jedem Urnengang durchgeführt. |
| **Zu minimieren** | Eine oder mehrere Massnahmen werden ergriffen, mit denen die Auswirkungen oder die Eintrittswahrscheinlichkeit eines Risikos reduziert werden sollen. Nach der Umsetzung der Massnahmen, wird das Restrisiko erneut identifiziert und beurteilt. Falls ein Risiko nicht wirksam minimiert werden kann, muss die Ausnahme von der Leitung der Staatskanzlei / Standeskanzlei begründet und ausdrücklich gutgeheissen werden. |
| **Abgewälzt** | Risiken werden durch einen Dritten getragen. Dieser reduziert das Schadensausmass für den Kanton (z.B. Abdeckung finanzieller Schäden durch eine Versicherung). Das Risikoportfolio enthält keine Risiken dieser Kategorie. |

Tabelle 4: Optionen für den Umgang mit Risiken

Wenn ein Risiko einen Lieferanten des Kantons betrifft, kann der Kanton die Umsetzung von Massnahmen an diesen delegieren. Der Kanton informiert die Lieferanten über alle Risiken, die einen Bezug zu ihnen haben und kontrolliert, dass allfällige Massnahmen umgesetzt werden.

# 10 Abbildungsverzeichnis



# 11 Tabellenverzeichnis