Risikoportfolio

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

Autor	Projektleitung E-Voting (BS) E-Voting Beauftragter (GR) Leitung der elektronischen Stimmabgabe (SG) Fachperson E-Voting (TG)
Datum	24.01.2024
Version	N/A
Klassifizierung	Keine

Prüf-/Freigabestellen

Prüfer	Freigeber	Datum
Leitung Recht und Volksrechte (BS)	Leitung Recht und Volksrechte (BS)	12.12.2022
Leitung Dienst für politische Rechte (SG)	Leitung Dienst für politische Rechte (SG)	12.12.2022
Leitung Rechtsdienst (TG)	Leitung Rechtsdienst (TG)	12.12.2022
Leitung Abteilung Services (GR)	Leitung Abteilung Services (GR)	22.09.2023

Blatt	Link	Name	Kantone	Sicherheitsziel	Problembereich	Informationsressourcen	Akteur	Ergebnis	Wahrscheinlichkeit	Risiko-Score	Risikostufe	Risikobehandlung	involvierte Dritte
GEN-R01	GEN-R01	GEN-R01 - Computer funktionieren nicht und die Operationen können nicht durchgeführt werden (Kanton)	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Durch Hardware oder Software Fehler können die für den Urnengang notwendigen Operationen nicht durchgeführt werden.	P08 - Codes (Initialisierungs-, Bestätigungs- und Finalisierungscode sowie Prüfcodes) P09 - Stimmrechtsausweise (inkl. Stimmregister nicht anonymisiert, Codes) P10 - Elektronische Stimme P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen P13 - Sensible Daten für den Verifier P14 - Ergebnisse des Verifiers / Papier-Protokolle / Technische Logs P15 - Software der Post beim Kanton (SDM, Verifier) P17 - Software von Abraxas beim Kanton (VOTING Stimmunterlagen; nur für SG)	Software/System	Abbruch	Gering	21	Signifikant	Akzeptiert	-
GEN-R02	GEN-R02	GEN-R02 - Infrastruktur der Post steht nicht zur Verfügung und die Operationen können nicht durchgeführt werden	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Die Infrastruktur der Post steht für die erforderlichen Operationen nicht zur Verfügung. Die entsprechenden Schritte können nicht durchgeführt werden.	P08 - Codes (Initialisierungs-, Bestätigungs- und Finalisierungscode sowie Prüfcodes) P10 - Elektronische Stimme P11 - Protokollierte Kontrollstimmen P13 - Sensible Daten für den Verifier P16 - Software der Post bei der Post (E-Voting Server, Kontrollkomponenten, usw.)	Software/System	Abbruch	Mittel	20	Signifikant	Akzeptiert	Post
GEN-R03	GEN-R03	GEN-R03 - Daten werden nicht oder nur teilweise vernichtet und offengelegt (Kanton)	Alle	Schutz der persönlichen Informationen über die Stimmberechtigten	Die Daten werden nach den Urnengang nicht (vollständig) vernichtet.	P02 - Parameter des Urnengangs / Gegenstand des Urnengangs / Mitglieder Admin-Board und Electoral-Board / SRA-Templates von VOTING Stimmunterlagen / Verschlüsselungsparameter / Abstimmungs- und Wahloptionen (Primzahlen) P10 - Elektronische Stimme P13 - Sensible Daten für den Verifier	Intern	Offenlegung	Gering	18	Gering	Akzeptiert	-
GEN-R04	GEN-R04	GEN-R04 - Daten werden nicht oder nur teilweise vernichtet und offengelegt (Post)	Alle	Schutz der persönlichen Informationen über die Stimmberechtigten	Die Daten werden nach den Urnengang nicht (vollständig) vernichtet.	P02 - Parameter des Urnengangs / Gegenstand des Urnengangs / Mitglieder Admin-Board und Electoral-Board / SRA-Templates von VOTING Stimmunterlagen / Verschlüsselungsparameter / Abstimmungs- und Wahloptionen (Primzahlen) P10 - Elektronische Stimme P13 - Sensible Daten für den Verifier	Extern	Offenlegung	Gering	18	Gering	Akzeptiert	Post
GEN-R05	GEN-R05	GEN-R05 - Änderung der Daten bei der Druckerei	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Durch veränderte Daten in der Druckerei können die Stimmberechtigen nicht abstimmen, oder die Gemeinden können die Doppelstimmprüfung nicht durchführen.	P09 - Stimmrechtsausweise (inkl. Stimmregister nicht anonymisiert, Codes)	Extern	Änderung	Gering	21	Signifikant	Zu überwachen	Druckerei
P01-R01	P01-R01	P01-R01 - Anpassung Informationswebseite	Alle	Schutz der für die Stimmberechtigten bestimmten Informationen vor Manipulationen	Anpassungen der Informationswebseite führen dazu, dass die Stimmberechtigten keinen Zugriff auf korrekte Informationen haben.	P01 - Hilfsmittel für die Stimmberechtigten	Intern	Änderung	Gering	14	Gering	Akzeptiert	-
P01-R02	P01-R02	P01-R02 - Die digitalen Erläuterungen stehen nicht mehr zur Verfügung	GR	N/A	Die Erläuterungen zu den Abstimmungsvorlagen werden digital vom Kanton bereitgestellt. Sie müssen den Stimmberechtigten während der Wahl- oder Abstimmungsphase zur Verfügung stehen.	P01 - Hilfsmittel für die Stimmberechtigten	System	Vernichtung / Verlust	Gering	16	Gering	Akzeptiert	-
P01-R03	P01-R03	P01-R03 - Phishing / Spoofing durch E-Mail des Kantons	GR	Schutz der für die Stimmberechtigten bestimmten Informationen vor Manipulationen	Die Stimmberechtigten können durch Phishing oder Spoofing beeinflusst werden (z.B. gefälschte Webseite).	P01 - Hilfsmittel für die Stimmberechtigten	Extern	Änderung	Gering	14	Gering	Akzeptiert	-
P02-R01	P02-R01	P02-R01 - Anpassung von Daten (Konfiguration/Stimmregister) stört den Urnengang	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Die Daten für die Konfiguration des Urnengangs werden durch Interne/Externe/SW-Fehler angepasst, was zu eine Störung des Urnengangs führt.	P02 - Parameter des Urnengangs / Gegenstand des Urnengangs / Mitglieder Admin-Board und Electoral-Board / SRA-Templates von VOTING Stimmunterlagen / Verschlüsselungsparameter / Abstimmungs- und Wahloptionen (Primzahlen) P03 - EV-Stimmregister (nicht anonymisiert) P04 - EV-Stimmregister (anonymisiert)	Intern/Extern/Software	Änderung	Gering	21	Signifikant	Akzeptiert	-
P02-R02	P02-R02	P02-R02 - Entnahme von sicherheitsrelevanten Daten	Alle	Schutz der persönlichen Informationen über die Stimmberechtigten	Durch Entnahme sind sicherheitsrelevante Konfigurationsdaten nicht mehr vertraulich.	P02 - Parameter des Urnengangs / Gegenstand des Urnengangs / Mitglieder Admin-Board und Electoral-Board / SRA-Templates von VOTING Stimmunterlagen / Verschlüsselungsparameter / Abstimmungs- und Wahloptionen (Primzahlen)	Extern	Offenlegung	Gering	20	Gering	Akzeptiert	-
P03-R01	P03-R01	P03-R01 - Offenlegung Stimmregister	Alle	Schutz der persönlichen Informationen über die Stimmberechtigten	Durch Offenlegung sind die im Stimmregister enthaltenen Daten nicht mehr vertraulich.	P03 - EV-Stimmregister (nicht anonymisiert) P18 - Register der Stimmrechtsausweise	Intern	Offenlegung	Gering	18	Gering	Akzeptiert	-
P04-R01	P04-R01	P04-R01 - Datenanpassung bei Anonymisierung des Stimmregisters	Alle	Schutz der persönlichen Informationen über die Stimmberechtigten	Die anonymisierten Simmregisterdaten sind nicht deckungleich mit den Quelldaten.	P04 - EV-Stimmregister (anonymisiert)	Software	Änderung	Gering	14	Gering	Akzeptiert	-
P04-R02	P04-R02	P04-R02 - Fehler bei Anonymisierung des Stimmregisters	Alle	Schutz der persönlichen Informationen über die Stimmberechtigten	Durch eine fehlerhafte Anonymisierung werden Personendaten offengelegt.	P03 - EV-Stimmregister (anonymisiert)	Software	Offenlegung	Gering	12	Gering	Akzeptiert	-
P07-R01	P07-R01	P07-R01 - Beide Passwörter sind einer Person bekannt	Alle	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse	Die Passwörter werden angewendet, um die Privat-Schlüssel der Urnen zu generieren. Wenn die zwei Passwörter bei einer Person zusammenkommen, ist es möglich, die Urnen zu entschlüsseln.	P07 - Passwörter des Urnengangs	Intern/Extern	Offenlegung	Gering	18	Gering	Akzeptiert	-
P07-R02	P07-R02	P07-R02 - Die Passwörter erlauben nicht, die Urnen zu entschlüsseln	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Die Passwörter müssen wie im D2 definiert eingegeben werden. Sonst kann der Privat-Schlüssel nicht korrekt generiert werden und die Urnen können nicht enschlüsselt werden.	P07 - Passwörter des Urnengangs	Intern/Extern	Offenlegung	Gering	21	Signifikant	Akzeptiert	-
P08-R01	P08-R01	P08-R01 - Offenlegung der Codes	Alle	Korrektheit des Ergebnisses / Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse	Mit den Codes kann ein Dritter für die Stimmberechtigten abstimmen Ein Dritter kann die Stimmabgabe von Wählenden manipulieren (Umgehung der individuellen und universellen Verifizierbarkeit, zB mit einer Schadsoftware auf der Plattform oder auf dem Server oder mit einem falschen Server)	P08 - Codes (Initialisierungs-, Bestätigungs- und Finalisierungscode sowie Prüfcodes) P09 - Stimmrechtsausweise (inkl. Stimmregister nicht anonymisiert, Codes)	Intern/Extern	Offenlegung	Gering	21	Signifikant	Zu überwachen	-
P08-R02	P08-R02	P08-R02 - Änderung der Codes	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Ohne die richtigen Codes können die Stimmberechtigten ihre Stimme nicht abgeben / kontrollieren / bestätigen.	P08 - Codes (Initialisierungs-, Bestätigungs- und Finalisierungscode sowie Prüfcodes) P09 - Stimmrechtsausweise (inkl. Stimmregister nicht anonymisiert, Codes)	Intern/Extern/Software	Änderung	Gering	21	Signifikant	Zu überwachen	-
P08-R03	P08-R03	P08-R03 - Änderung der Codes durch die Post	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Ohne die richtigen Codes können die Stimmberechtigten ihre Stimme nicht abgeben / kontrollieren / bestätigen.	P08 - Codes (Initialisierungs-, Bestätigungs- und Finalisierungscode sowie Prüfcodes)	Extern/Software	Änderung	Gering	21	Signifikant	Zu überwachen	Post

P09-R01	P09-R01	P09-R01 - Offenlegung der SRAs in der Druckerei	Alle	Korrektheit des Ergebnisses / Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse	Durch Zugang zu den Stimmrechtsausweise werden die Codes offengelegt, wodurch ein Dritter für die Stimmberechtigten abstimmen kann.	P09 - Stimmrechtsausweise (inkl. Stimmregister nicht anonymisiert, Codes)	Extern	Offenlegung	Gering	21	Signifikant	Zu überwachen	Druckerei
P09-R02	P09-R02	P09-R02 - Verzögerung bei Druck und Versand der SRAs	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Ein Verlust der Daten auf den Datenträgern oder ein Problem bei der Druckerei führt dazu, dass einige Operationen wiederholt werden müssen.	P09 - Stimmrechtsausweise (inkl. Stimmregister nicht anonymisiert, Codes)	Intern/Extern/Hardware	Vernichtung / Verlust	Gering	13	Gering	Akzeptiert	-
P10-R01	P10-R01	P10-R01 - Verletzung des Stimmgeheimnisses	Alle	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse	Durch eine fehlerhafte Handhabung der Daten für die Prüfung oder durch Verwendung der Sicherheitsschlüssel des Urnengangs kann das Stimmgeheimnis gebrochen werden.	P10 - Elektronische Stimme	Intern	Offenlegung	Gering	18	Gering	Akzeptiert	-
P10-R02	P10-R02	P10-R02 - Stimmen werden an Dritte geschickt / von Dritten gelesen	Alle	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse	Durch eine Malware auf der Benutzerplattform kann das Stimmgeheimnis gebrochen werden.	P10 - Elektronische Stimme	Extern	Offenlegung	Gering	18	Gering	Akzeptiert	-
P10-R03	P10-R03	P10-R03 - Veränderung der Stimmen zwischen den Geräten der Stimmberechtigten und Server	Alle	Korrektheit des Ergebnisses	Die Stimme wird angepasst, bevor sie auf dem Server gespeichert wird.	P10 - Elektronische Stimme	Extern	Änderung	Gering	19	Gering	Akzeptiert	-
P10-R04	P10-R04	P10-R04 - Manipulation der Stimmen innerhalb der Post	Alle	Korrektheit des Ergebnisses	Die Stimme wird bei der Post verändert.	P10 - Elektronische Stimme	Extern	Änderung	Gering	21	Signifikant	Zu überwachen	Post
P10-R05	P10-R05	P10-R05 - Manipulation der Stimmen innerhalb des Kantons	Alle	Korrektheit des Ergebnisses	Durch eine interne Manipulation werden die Stimmen falsch auf dem Server gespeichert.	P10 - Elektronische Stimme	Intern	Änderung	Gering	20	Gering	Akzeptiert	-
P10-R06	P10-R06	P10-R06 - Codes werden von stimmberechtigten Personen nicht verifiziert	Alle	Schutz der für die Stimmberechtigten bestimmten Informationen vor Manipulationen	Ohne Verifikation der Codes durch die stimmberechtigten Personen, ist die individuelle Verifizierbarkeit nicht gegeben.	P10 - Elektronische Stimme	Extern	Änderung	Gering	18	Gering	Akzeptiert	-
P10-R07	P10-R07	P10-R07 - Stimmen können ohne Entschlüsselung gelesen werden	Alle	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse	Durch ein Problem im Verschlüsselungsprozess wird das Stimmgeheimnis gebrochen.	P10 - Elektronische Stimme	Intern/Extern/Software	Offenlegung	Gering	18	Gering	Akzeptiert	-
P10-R08	P10-R08	P10-R08 - Anpassungen von Stimmen, ohne dass dies von der universellen Verifizierbarkeit bemerkt wird	Alle	Korrektheit des Ergebnisses	Die Wirkung der universellen Verifizierbarkeit ist zentral für das Vertrauen in den Urnengang.	P10 - Elektronische Stimme	Software	Änderung	Gering	20	Gering	Akzeptiert	-
P10-R09	P10-R09	P10-R09 - Stimmen können nicht entschlüsselt werden	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Ohne Entschlüsselung (z.B. Problem mit der Kryptographie) ist es nicht möglich, die Stimmen auszuzählen.	P10 - Elektronische Stimme	Software	Abbruch	Gering	21	Signifikant	Zu überwachen	-
P10-R10	P10-R10	P10-R10 - Fehler bei der individuellen Verifizierbarkeit	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Die individuelle Verifizierbarkeit ist nicht mehr stichhaltig.	P10 - Elektronische Stimme	Software	Abbruch	Gering	19	Gering	Akzeptiert	-
P10-R11	P10-R11	P10-R11 - Stimmenkauf durch Angreifer	Alle	keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten	Die Wahl- / Stimmfreiheit ist nicht gewährleistet.	P10 - Elektronische Stimme	Intern/Extern	Änderung	Gering	14	Gering	Akzeptiert	-
P10-R12	P10-R12	P10-R12 - Beinflussung der Meinungsbildung	Alle	keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten	Die Stimme im System entspricht durch Beeinflussung nicht der intrinsischen Meinung des Stimmberechtigten.	P10 - Elektronische Stimme	Extern	Änderung	Gering	20	Gering	Akzeptiert	-
P10-R13	P10-R13	P10-R13 - Stimmabgabe ist durch Malware nicht möglich	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Durch Malware können die Stimmberechtigen ihre elektronische Stimme nicht auf der Benutzerplattform abgeben.	P10 - Elektronische Stimme	Extern	Abbruch	Gering	18	Gering	Akzeptiert	-
P11-R01	P11-R01	P11-R01 - Protokolle der Kontrollstimmen stehen nicht zur Verfügung	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Ohne die Protokolle der einzelnen Stimmen der Kontrollurne kann die Kontrolle am D3 nicht stattfinden.	P11 - Protokollierte Kontrollstimmen	Intern/Extern	Vernichtung / Verlust	Gering	14	Gering	Akzeptiert	-
P11-R02	P11-R02	P11-R02 - Protokolle der Kontrollstimmen stimmen mehrheitlich nicht mit den Ergebnissen überein	Alle	Korrektheit des Ergebnisses	Die Protokolle der einzelnen Stimmen stimmen nicht mit den Ergebnissen der Kontrollurne überein.	P11 - Protokollierte Kontrollstimmen	Intern/Extern	Änderung	Gering	10	Gering	Akzeptiert	-
P12-R01	P12-R01	P12-R01 - EV-Ergebnisse werden gelöscht, bevor sie ins Ergebnisermittlungssystem eingespielt werden	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Durch Löschung der Ergebnisse können diese nicht ausgezählt werden.	P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen	Intern	Vernichtung / Verlust	Gering	11	Gering	Akzeptiert	-
P12-R02	P12-R02	P12-R02 - Vorzeitige Offenlegung der EV-Ergebnisse	Alle	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse	Die Ergebnisse werden vor Abschluss der Abstimmungsphase offengelegt.	P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen	Intern/Extern	Offenlegung	Gering	14	Gering	Akzeptiert	-
P12-R03	P12-R03	P12-R03 - EV-Ergebnisse werden geändert, bevor sie in Ergebnisermittlungssystem eingespielt werden	Alle	Korrektheit des Ergebnisses	Es werden fehlerhafte Ergebnisse publiziert.	P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen	Intern/Extern/Software	Änderung	Gering	11	Gering	Akzeptiert	-
P12-R04	P12-R04	P12-R04 - EV-Ergebnisse werden nicht korrekt gezählt	Alle	Korrektheit des Ergebnisses	Durch falsch ausgezählte Ergebnisse werden fehlerhafte Daten publiziert.	P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen	Software	Änderung	Gering	19	Gering	Akzeptiert	-
P13-R01	P13-R01	P13-R01 - Fehler oder Anomalie bei der Überprüfung der Ergebnisse	Alle	Korrektheit des Ergebnisses	Der Verifier weist Fehler aus.	P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen P13 - Sensible Daten für den Verifier	Intern/Extern/Software	Abbruch	Gering	21	Signifikant	Zu überwachen	-
P13-R02	P13-R02	P13-R02 - Verifier kann nicht oder nur teilweise eingesetzt werden	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Die universelle Verifizierbarkeit ist nicht mehr stichhaltig.	P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen P13 - Sensible Daten für den Verifier	Software	Abbruch	Gering	19	Gering	Akzeptiert	-
P14-R01	P14-R01	P14-R01 - Änderung der technischen Logs	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Durch Änderung oder Löschung der technischen Logs liefern die Untersuchungen falsche Ergebnisse.	P14 - Ergebnisse des Verifiers / Papier-Protokolle / Technische Logs	Intern/Extern	Änderung	Gering	20	Gering	Akzeptiert	-
P14-R02	P14-R02	P14-R02 - Änderung der technischen Logs bei der Post	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Durch Änderung oder Löschung der technischen Logs liefern die Untersuchungen falsche Ergebnisse.	P14 - Ergebnisse des Verifiers / Papier-Protokolle / Technische Logs	Extern	Änderung	Gering	20	Gering	Akzeptiert	Post
P14-R03	P14-R03	P14-R03 - Fehlende Papier-Protokolle	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Durch Löschung der Protokolle fehlt ein Mittel für allfällige Untersuchungen.	P14 - Ergebnisse des Verifiers / Papier-Protokolle / Technische Logs	Intern/Extern	Vernichtung / Verlust	Gering	16	Gering	Akzeptiert	-
P15-R01	P15-R01	P15-R01 - Falsche Software installiert (Kanton)	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Mit der falschen Software wird den Urnengang nicht korrekt ablaufen oder anfällig für Manipulationen sein.	P15 - Software der Post beim Kanton (DIS, SDM, Verifier) P17 - Software von Abraxas beim Kanton (VOTING Stimmunterlagen; nur für SG)	Intern	Änderung	Gering	11	Gering	Akzeptiert	-
P15-R02	P15-R02	P15-R02 - Manipulation von Software (Kanton)	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Durch die Manipulation von Software wird der Urnengang nicht korrekt ablaufen.	P15 - Software der Post beim Kanton (DIS, SDM, Verifier) P17 - Software von Abraxas beim Kanton (VOTING Stimmunterlagen; nur für SG)	Extern	Änderung	Gering	19	Gering	Zu minimieren	-
P16-R01	P16-R01	P16-R01 - Falsche Software installiert (Post)	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Mit der falschen Software wird den Urnengang nicht korrekt ablaufen oder anfällig für Manipulationen sein.	P16 - Software der Post bei der Post (E-Voting Server, Kontrollkomponenten, usw.)	Extern	Änderung	Gering	11	Gering	Akzeptiert	Post

P16-R02	P16-R02	P16-R02 - Manipulation von Software (Post)	Alle	Korrektheit des Ergebnisses	Durch eine Manipulation der Software wird der Urnengang manipuliert.	P16 - Software der Post bei der Post (E-Voting Server, Kontrollkomponenten, usw.)	Extern	Änderung	Gering	20	Gering	Akzeptiert	-
P16-R03	P16-R03	P16-R03 - Nutzbare Schwachstellen in der Software der Post	Alle	Korrektheit des Ergebnisses	In der Software der Post existieren nutzbare Schwachstellen.	P15 - Software der Post beim Kanton (DIS, SDM, Verifier) P16 - Software der Post bei der Post (E-Voting Server, Kontrollkomponenten, usw.)	Extern	Änderung	Gering	20	Gering	Akzeptiert	Post
P18-R01	P18-R01	P18-R01 - Änderung des Registers der Stimmrechtsausweise	Alle	Korrektheit des Ergebnisses	Ohne die richtige Verbindung zwischen dem Register der Stimmberechtigten und den Stimmrechtsausweisen könnte bei der Erstellung von Duplikaten Fehler auftreten.	P18 - Register der Stimmrechtsausweise	Intern/Extern/Software	Änderung	Gering	14	Gering	Akzeptiert	-
P19-R01	P19-R01	P19-R01 - Kompromittierte Signaturzertifikate	Alle	Korrektheit des Ergebnisses	Die Signaturzertifikate sind durch Anpassung oder Offenlegung kompromittiert und können nicht mehr verwendet werden. Die Kommunikationskanäle sind nicht mehr vertrauenswürdig.	P19 - Signaturzertifikate	Intern/Extern	Vernichtung / Verlust	Gering	11	Gering	Akzeptiert	-
P20-R01	P20-R01	P20-R01 - Quorum des Admin-Boards kann nicht erreicht werden	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Ohne die Passwörter des Admin-Boards können die Aufgaben der Mitglieder des Admin-Boards (D1, D2 und D3) nicht durchgeführt werden. Insb. ist es nicht mehr möglich, die Urnen vorzubereiten oder zu entschlüsseln.	P20 - Passwörter des Admin-Boards (Profil)	Intern/Extern	Vernichtung / Verlust	Gering	21	Signifikant	Zu überwachen	-
P20-R02	P20-R02	P20-R02 - Die Passwörter sind offengelegt	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Das persönliche Passwort muss geheim bleiben, damit das 4-Augen-Prinzip gewährleistet ist.	P20 - Passwörter des Admin-Boards (Profil)	Intern/Extern	Offenlegung	Gering	11	Gering	Akzeptiert	-
RPA-01	RPA-01	RPA-01 - Beschwerde gegen Kanton wegen ungenügenden Sicherheitsmassnahmen	Alle	N/A	Gegen einen Kanton wird Beschwerde eingereicht, weil er ein System betrieben und dabei ungenügende Sicherheitsmassnahmen ergriffen hat.	N/A	N/A	N/A	Gering	17	Gering	Akzeptiert	-
RPA-03	RPA-03	RPA-03 - Streitigkeiten zwischen den Behörden und der Post	Alle	N/A	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.	N/A	N/A	N/A	Gering	14	Gering	Akzeptiert	-
RPA-04	RPA-04	RPA-04 - Untersuchung eines Angriffs kann nicht ordentlich durchgeführt werden	Alle	N/A	Die Untersuchung eines Angriffs auf dem elektronischen Stimmkanal kann wegen fehlender technischer Möglichkeiten nicht ordentlich durchgeführt werden.	N/A	N/A	N/A	Gering	18	Gering	Akzeptiert	-
RPA-05	RPA-05	RPA-05 - Angriff kann nicht verfolgt werden	Alle	N/A	Ein Angriff auf den elektronischen Stimmkanal kann wegen fehlender rechtlicher Möglichkeiten nicht verfolgt werden.	N/A	N/A	N/A	Gering	14	Gering	Akzeptiert	-
RPA-06	RPA-06	RPA-06 - Kampagne gegen E-Voting	Alle	N/A	In den Medien oder in sozialen Netzwerken wird eine Kampagne gegen den elektronischen Stimmkanal geführt. Sie kann auf Geschehnisse rund um die elektronische Stimmabgabe im Ausland oder auf fehlende öffentliche Kontrollmöglichkeiten abzielen; denkbar ist auch, dass die Mechanismen der Verifizierbarkeit instrumentalisiert werden oder den Behörden mangelnde Kommunikation vorgeworfen wird.	N/A	N/A	N/A	Mittel	14	Signifikant	Zu überwachen	-
RPA-07	RPA-07	RPA-07 - Abweichung EV-Ergebnisse zu anderen Kanälen	Alle	N/A	Bei der Auszählung stellt sich heraus, dass die Ergebnisse der elektronischen Stimmabgabe von den Ergebnissen der anderen Stimmkanäle abweichen.	N/A	N/A	N/A	Gering	16	Gering	Akzeptiert	-
RPA-08	RPA-08	RPA-08 - Fehlende Ressourcen	Alle	N/A	Den Kantonen fehlen die Ressourcen für die Umsetzung des elektronischen Stimmkanals.	N/A	N/A	N/A	Gering	14	Gering	Akzeptiert	-
RPA-09	RPA-09	RPA-09 - Kampagne zum Stimmenkauf	Alle	N/A	Eine Gruppe, die über eine anonyme Kaufplattform verfügt, lanciert eine grossangelegte Kampagne zum Stimmenkauf.	N/A	N/A	N/A	Gering	14	Gering	Akzeptiert	-
RPA-10	RPA-10	RPA-10 - Reaktion auf Sicherheitsvorfall	Alle	N/A	Während der Phase der Stimmabgabe ereignet sich ein sicherheitsrelevanter Vorfall und es wird nicht innert nützlicher Frist adäquat reagiert.	N/A	N/A	N/A	Gering	14	Gering	Akzeptiert	-
RPA-11	RPA-11	RPA-11 - Ergebnisse können nicht rechtzeitig bestätigt werden	Alle	N/A	Wenn der Verifier einen Fehler oder eine Anomalie ausgibt, muss die Ursache analysiert werden. Wenn die Analyse zu lange dauert, wird zum Zeitpunkt der Publikation nicht bekannt sein, ob die Ergebnisse der elektronischen Urnen ermittelt werden können.	N/A	N/A	N/A	Gering	23	Signifikant	Zu überwachen	-
RPA-12	RPA-12	RPA-12 - Ein Ausfall des Voter-Portals verhindert der Stimmabgabe	GR	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Wegen einen Systemausfalls können gewisse Gruppen nicht abstimmen, da das Material für die briefliche Abstimmung nicht rechtzeitig ankommt.	N/A	N/A	N/A	Gering	16	Gering	Akzeptiert	-
RPA-13	RPA-13	RPA-13 - Anmeldung durch Dritte durchgeführt	GR	N/A	Eine Drittperson meldet Stimmberechtigte für E-Voting an.	N/A	N/A	N/A	Gering	20	Gering	Akzeptiert	-

RPA-01 - Beschwerde gegen Kanton wegen ungenügenden Sicherheitsmassnahmen

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	N/A

Bedrohung

Informationsressourcen	N/A
Problembereich	Gegen einen Kanton wird Beschwerde eingereicht, weil er ein System betrieben und dabei ungenügende Sicherheitsmassnahmen ergriffen hat.
(1) Akteur Wer wird die Bedrohung ausnutzen?	N/A
(2) Mittel Wie wird der Akteur vorgehen?	N/A
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die Beschwerde wird ein mediales Echo auslösen und es werden Untersuchungen lanciert, um die Sicherheitsmassnahmen zu analysieren.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**17**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch die Umsetzung der Anforderungen der VEleS ist eine Beschwerde unwahrscheinlich, da diese nicht substanziert werden könnte.
Dazu ist die Konformität mit der VEleS im Vertrag mit der Post explizit aufgenommen. Der Kanton führt E2E-Tests durch und verfolgt eng die Überprüfung des Systems durch die Bundeskanzlei.
Produktivität: Wir gehen nicht davon aus, dass die Arbeitsbelastung um mehr als 20 bis 50% steigen würde, daher als "Mittel" eingestuft.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

RPA-03 - Streitigkeiten zwischen den Behörden und der Post

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		N/A
Bedrohung	**Informationsressourcen**	N/A
	Problembereich	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.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	N/A
	(2) Mittel Wie wird der Akteur vorgehen?	N/A
	(3) Motivation Warum tut er das?	N/A
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch**
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?	**(8) Schwere** Wie schwer ist der Schaden je Risikobewertungskriterium?		
	Kriterium	**Kritikalität**	**Score**
Die elektronische Stimmabgabe wird gestoppt, was die Reputation für die betroffenen Kantonen beeinträchtigt, die sich für die Post entschieden haben.	Reputation und Vertrauen	Mittel	8
	Finanzen	Tief	3
	Produktivität	Tief	1
	Gesundheit und Sicherheit	N/A	0
	Rechtliches	Tief	2
	Andere	N/A	0
		Risiko-Score	**14**
		Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

vgl. dazu auch Risikobeurteilung der Bundeskanzlei ("BK-VE-R16 Wegfall Stimmkanal wegen unzureichender Zusammenarbeit")

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

RPA-04 - Untersuchung eines Angriffs kann nicht ordentlich durchgeführt werden

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	N/A

Bedrohung

Informationsressourcen	N/A
Problembereich	Die Untersuchung eines Angriffs auf dem elektronischen Stimmkanal kann wegen fehlender technischer Möglichkeiten nicht ordentlich durchgeführt werden.
(1) Akteur Wer wird die Bedrohung ausnutzen?	N/A
(2) Mittel Wie wird der Akteur vorgehen?	N/A
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Wenn die Untersuchungen nicht sachgemäss durchgeführt werden, verursacht dies Reputationsschäden.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**18**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Erfahrungen des letzten produktiven Urnengangs und der Tests haben gezeigt, dass die Post gute Informationen liefern kann (Bsp. Begleitgruppentests 2018).

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers
	Die Forensic Readiness wird nach dem produktiven Einsatz in Zusammenarbeit mit der Bundeskanzlei ausgebaut (vgl. Massnahmenkatalog B.13).		

RPA-05 - Angriff kann nicht verfolgt werden

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	N/A

Bedrohung

Informationsressourcen	N/A
Problembereich	Ein Angriff auf den elektronischen Stimmkanal kann wegen fehlender rechtlicher Möglichkeiten nicht verfolgt werden.
(1) Akteur Wer wird die Bedrohung ausnutzen?	N/A
(2) Mittel Wie wird der Akteur vorgehen?	N/A
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Es könnte, je nach Auslöser, zu Reputationsschäden kommen (beispielsweise beim Fehlen von rechtlichen Grundlagen).

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
Risiko-Score		**14**
Risiko-Stufe		**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

RPA-06 - Kampagne gegen E-Voting

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	N/A

Bedrohung

Informationsressourcen	N/A
Problembereich	In den Medien oder in sozialen Netzwerken wird eine Kampagne gegen den elektronischen Stimmkanal geführt. Sie kann auf Geschehnisse rund um die elektronische Stimmabgabe im Ausland oder auf fehlende öffentliche Kontrollmöglichkeiten abzielen; denkbar ist auch, dass die Mechanismen der Verifizierbarkeit instrumentalisiert werden oder den Behörden mangelnde Kommunikation vorgeworfen wird.
(1) Akteur Wer wird die Bedrohung ausnutzen?	N/A
(2) Mittel Wie wird der Akteur vorgehen?	N/A
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
	X	

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Das Vertrauen in die elektronische Stimmabgabe kann langfristig sinken.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**14**
	Risiko-Stufe	**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Kantone informieren über E-Voting, insb. durch die Informationsplattform.
Bund und Kantone haben insb. auch mit der Neuausrichtung viele Massnahmen getroffen, um das Vertrauen der Öffentlichkeit zu verdienen. Diese Massnahmen können aufgezeigt werden.
vgl. dazu auch Risikobeurteilung der Bundeskanzlei ("BK-VE-R4 Negativkampagne gegen E-Voting in (sozialen) Medien")

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
	X			

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers
		-	-

RPA-07 - Abweichung EV-Ergebnisse zu anderen Kanälen

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	N/A

Bedrohung

Informationsressourcen	N/A
Problembereich	Bei der Auszählung stellt sich heraus, dass die Ergebnisse der elektronischen Stimmabgabe von den Ergebnissen der anderen Stimmkanäle abweichen.
(1) Akteur Wer wird die Bedrohung ausnutzen?	N/A
(2) Mittel Wie wird der Akteur vorgehen?	N/A
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Der Vertrauen in die elektronische Stimmabgabe kann langfristig sinken.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**16**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

In der Vergangenheit (100 Urnengänge) wurde keine bedeutenden Abweichung festgestellt.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

RPA-08 - Fehlende Ressourcen

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	N/A

Bedrohung

Informationsressourcen	N/A
Problembereich	Den Kantonen fehlen die Ressourcen für die Umsetzung des elektronischen Stimmkanals.
(1) Akteur Wer wird die Bedrohung ausnutzen?	N/A
(2) Mittel Wie wird der Akteur vorgehen?	N/A
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die Kantone werden die elektronische Stimmabgabe nicht einführen und die Post wird E-Voting wegen nicht erreichbarem Business Case stoppen.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
Risiko-Score		**14**
Risiko-Stufe		**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Das Budget ist aufgrund der Kosten und der nötigen Ressourcen eingestellt.
vgl. dazu auch Risikobeurteilung der Bundeskanzlei ("BK-VE-R17 Wegfall Stimmkanal wegen fehlender Ressourcen")

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

RPA-09 - Kampagne zum Stimmenkauf

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	N/A

Bedrohung

Informationsressourcen	N/A
Problembereich	Eine Gruppe, die über eine anonyme Kaufplattform verfügt, lanciert eine grossangelegte Kampagne zum Stimmenkauf.
(1) Akteur Wer wird die Bedrohung ausnutzen?	N/A
(2) Mittel Wie wird der Akteur vorgehen?	N/A
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Durch die Kaufplattform würde die Reputation von E-Voting sinken.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**14**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

vgl. dazu auch Risikobeurteilung der Bundeskanzlei ("BK-VE-R5 Stimmenkauf über anonyme Plattform")

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

RPA-10 - Reaktion auf Sicherheitsvorfall

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	N/A

Bedrohung

Informationsressourcen	N/A
Problembereich	Während der Phase der Stimmabgabe ereignet sich ein sicherheitsrelevanter Vorfall und es wird nicht innert nützlicher Frist adäquat reagiert.
(1) Akteur Wer wird die Bedrohung ausnutzen?	N/A
(2) Mittel Wie wird der Akteur vorgehen?	N/A
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A

(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	Hoch	Mittel	Gering
			X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die Medienberichte werden kritisch gegenüber E-Voting sein und der Urnengang wird in Frage gestellt. Die Bundeskanzlei kommuniziert eingenständig ohne Abstimmung mit den Kantonen.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**14**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch Krisenszenarien und die Krisenvereinbarung werden solche Szenarien vorbereitet.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

RPA-11 - Ergebnisse können nicht rechtzeitig bestätigt werden

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		N/A
Bedrohung	**Informationsressourcen**	N/A
	Problembereich	Wenn der Verifier einen Fehler oder eine Anomalie ausgibt, muss die Ursache analysiert werden. Wenn die Analyse zu lange dauert, wird zum Zeitpunkt der Publikation nicht bekannt sein, ob die Ergebnisse der elektronischen Urnen ermittelt werden können.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	N/A
	(2) Mittel Wie wird der Akteur vorgehen?	N/A
	(3) Motivation Warum tut er das?	N/A
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch**
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Am Sonntag werden die EV-Ergebnisse nicht berücksichtigt, da die Analysen noch nicht abgeschlossen werden konnten. Die am Sonntag publizierten Ergebnisse weichen von den bestätigten Ergebnissen ab.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Hoch	6
Andere	N/A	0
	Risiko-Score	**23**
	Risiko-Stufe	**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Kritisch ist dies inbesondere bei Abstimmungen oder Wahlen mit knappen Resultaten. Da das Elektorat bei E-Voting gering ist, ist die Wahrscheinlichkeit, dass ein Resultat gekippt werden könnte, klein.
Die Kantone, die am Samstag den Urnengang durch den Verifier überprüfen, haben mehr Zeit, um die Ursache zu untersuchen.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
	X			

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

RPA-12 - Ein Ausfall des Voter-Portals verhindert der Stimmabgabe

Risiko

Betroffene Kantone		GR
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Bedrohung	**Informationsressourcen**	N/A
	Problembereich	Wegen einen Systemausfalls können gewisse Gruppen nicht abstimmen, da das Material für die briefliche Abstimmung nicht rechtzeitig ankommt.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	N/A
	(2) Mittel Wie wird der Akteur vorgehen?	N/A
	(3) Motivation Warum tut er das?	N/A
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch**
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Verfügbarkeit des Systems wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering**: X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Ein Auslandschweizer / eine Auslandschweizerin reicht eine Beschwerde ein, weil er im Ausnahmenfall (z.B. Total-Ausfall des E-Voting-Systems) nicht abstimmen kann.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**16**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Beurteilung der Wahrscheinlichkeit und der Auswirkung erfolgte aufgrund der folgenden getroffenen Massnahmen:
- Das Gesetz (GPR) definiert die Auswirkungen einer E-Voting-Anmeldung klar.
- Die Stimmberechtigten werden vor der E-Voting-Anmeldung über deren Auswirkung klar informiert.

Des Weiteren überwiegen die Vorteile von E-Voting für die Auslandschweizer/-innen gegenüber den konventionalen Stimmkanälen.
Die Gemeinden stellen sicher, dass genügend physisches Stimmmaterial zur Verfügung steht, damit E-Voter Ersatzmaterial bestellen können oder an der Urne abstimmen können (für den Fall, dass es die räumlichen Gegebenheiten zulassen).

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

RPA-13 - Anmeldung durch Dritte durchgeführt

Risiko

Betroffene Kantone		GR
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		N/A
Bedrohung	**Informationsressourcen**	N/A
	Problembereich	Eine Drittperson meldet Stimmberechtigte für E-Voting an.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	N/A
	(2) Mittel Wie wird der Akteur vorgehen?	N/A
	(3) Motivation Warum tut er das?	N/A
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch**
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Eine Drittperson meldet eine stimmberechtigte Person für E-Voting an. Die stimmberechtigte Person erhält folglich nur das Stimmmaterial für die elektronische Stimmabgabe. Die Drittperson spricht öffentlich darüber, was Reputationsschäden in Bezug auf das Modell des Kantons Graubünden verursacht.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**20**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Bei jeder Anmeldung wird eine schriftliche Bestätigung an die amtliche Adresse der stimmberechtigten Person verschickt. Dadurch wird die stimmberechtigte Person in Kenntnis gesetzt, dass etwas nicht korrekt vonstattenging. Den stimmberechtigten Personen wird bei Unsicherheiten/Unstimmigkeiten generell empfohlen, Kontakt mit der Gemeinde aufzunehmen.
Wenn die stimmberechtigte Person die schriftliche Bestätigung nicht erhalten sollte, erhält sie auf Anfrage bei der Gemeinde das Stimmaterial für die Stimmabgabe an der Urne oder per Brief.
Eine Abmeldung ist jederzeit möglich.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

GEN-R01 - Computer funktionieren nicht und die Operationen können nicht durchgeführt werden (Kanton)

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals

Bedrohung

Informationsressourcen	P08 - Codes (Initialisierungs-, Bestätigungs- und Finalisierungscode sowie Prüfcodes) P09 - Stimmrechtsausweise (inkl. Stimmregister nicht anonymisiert, Codes) P10 - Elektronische Stimme P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen P13 - Sensible Daten für den Verifier P14 - Ergebnisse des Verifiers / Papier-Protokolle / Technische Logs P15 - Software der Post beim Kanton (SDM, Verifier) P17 - Software von Abraxas beim Kanton (VOTING Stimmunterlagen; nur für SG)
Problembereich	Durch Hardware oder Software Fehler können die für den Urnengang notwendigen Operationen nicht durchgeführt werden.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Software/System
(2) Mittel Wie wird der Akteur vorgehen?	Durch Hardware oder Software Fehler funktionieren die Computer nicht und dadurch können die notwendigen Operationen nicht durchgeführt werden.
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**
	X

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Verfügbarkeit der Systeme (inkl. Informationsressourcen) wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die für den Urnengang notwendigen Schritte können nicht durchgeführt werden, was bedeutet, dass die elektronische Stimmabgabe gestoppt werden muss. Die elektronischen Stimmen können nicht ausgezählt werden. Es kommt zu landesweiten Medienberichten.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**21**
	Risiko-Stufe	**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch Urnengangtests (E2E-Tests vor jedem Urnengang auf den produktiven Geräten) wird die Wahrscheinlichkeit des Risikos minimiert.
Die Kantone verfügen über Reserve-Geräte im Fall von Hardware-Ausfällen. Mit den regelmässigen Backups der Geräte wird sichergestellt, dass der Prozess wieder aufgenommen werden kann.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers
Computer	Die Kantone haben je einen zusätzlichen produktiven Offline- und Online-Computer als Backup.		-

GEN-R02 - Infrastruktur der Post steht nicht zur Verfügung und die Operationen können nicht durchgeführt werden

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals

Bedrohung

Informationsressourcen	P08 - Codes (Initialisierungs-, Bestätigungs- und Finalisierungscode sowie Prüfcodes) P10 - Elektronische Stimme P11 - Protokollierte Kontrollstimmen P13 - Sensible Daten für den Verifier P16 - Software der Post bei der Post (E-Voting Server, Kontrollkomponenten, usw.)
Problembereich	Die Infrastruktur der Post steht für die erforderlichen Operationen nicht zur Verfügung. Die entsprechenden Schritte können nicht durchgeführt werden.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Software/System
(2) Mittel Wie wird der Akteur vorgehen?	Durch Hardware oder Software Fehler funktioniert die Infrastruktur der Post nicht und dadurch können die notwendigen Operationen nicht durchgeführt werden. Ein technischer Fehler des Systems führt dazu, dass das System zum Zeitpunkt der Auszählung nicht verfügbar ist. (LF 13.33) Durch einer Naturkatastophe steht ein Rechenzentrum der Post nicht mehr zur Verfügung. Eine feindliche Organisation führt einen Denial-of-Service-Angriff (DOSAngriff) durch. (LF 13.30)
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**
	X

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Verfügbarkeit der Systeme (inkl. Informationsressourcen) wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
	X	

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die für den Urnengang notwendigen Schritte können nicht durchgeführt werden, was bedeutet, dass die elektronische Stimmabgabe gestoppt werden muss. Die elektronischen Stimmen können nicht ausgezählt werden. Es kommt zu landesweiten Medienberichten.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**20**
	Risiko-Stufe	**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch Releasetests sowie Urnengangtests (E2E-Tests vor jedem Urnengang auf den produktiven Geräten) wird die Wahrscheinlichkeit des Risikos minimiert. Sowohl die Post (Splunk-Reporting und Überwachung der Infrasstruktur) als auch die Kantone (Abgabe von Teststimmen und Überwachung der Anfragen an die Supportstelle) führen ein Monitoring während des Abstimmungs- oder Wahlzeitraums durch, um allfällige Ausfälle früh zu erkennen.
DDoS-Angriffe: Die Eintretenswahrscheinlichkeit wird von gering auf mittel erhöht aufgrund der Erfahrungen mit der DDoS-Angriffswelle im Juni 2023. Die Auswirkungen werden belassen. Die Post verfügt über ein mehrstufiges technisches Abwehrdispositiv gegen DDOS-Angriffe. Ein spezialisiertes Team ist bei einem Angriff rund um die Uhr im Einsatz, um Abwehrmassnahmen umzusetzen. Zudem ist die Post als nationale kritische Infrastruktur eng im Nationalen Cybersicherheits-Kompetenzzentrum (NCSC) eingebunden und stimmt die Abwehrmassnahmen mit den Cybersecurity-Spezialisten des Bundes wie auch mit den Kantonen ab. Durch präventive Massnahmen kann die Wahrscheinlichkeit eines Systemausfalls im Fall eines Angriffs deutlich reduziert werden. Bei einem erfolgreichen Angriff stehen ebenfalls Massnahmen zur Verfügung, um die Verfügbarkeit möglichst rasch wiederherzustellen (Geo-Blocking). Nach der Urnenschliessung können zusätzliche Schutzmassnahmen umgesetzt werden, um die Verfügbarkeit des Systems für das Online-Mischen und Herunterladen der Urnen am Tag 3 sicherzustellen.
Die Kantone haben mit der Post ein SLA abgeschlossen, welches die Reakations- und Behebungszeiten definiert. Die Einhaltung des SLA wird nach jedem Urnengang kontrolliert. Die Kantone haben jederzeit das Recht, Informationen über die Umsetzung von Anforderungen zu erhalten oder die Umsetzung vor Ort zu kontrollieren. Die Kantone stehen in engem Austausch mit der Post und begleiten deren Arbeit. Die Kantone sind dadurch in der Lage, die Arbeit der Post zu beurteilen und nötigenfalls Einfluss zu nehmen.
Graubünden: Ein Total-Ausfall des Systems währen des Abstimmungs- oder Wahlzeitraums ist zusätzlich im Risiko RPA-12 adressiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				Post

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers
Computer	Die Kantone haben je einen zusätzlichen produktiven Offline- und Online-Computer als Backup.		-
Infrastruktur der Post	Präventive Massnahmen der Post gegen DDos-Angriffe		

GEN-R03 - Daten werden nicht oder nur teilweise vernichtet und offengelegt (Kanton)

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Schutz der persönlichen Informationen über die Stimmberechtigten

Bedrohung

Informationsressourcen	P02 - Parameter des Urnengangs / Gegenstand des Urnengangs / Mitglieder Admin-Board und Electoral-Board / SRA-Templates von VOTING Stimmunterlagen / Verschlüsselungsparameter / Abstimmungs- und Wahloptionen (Primzahlen) P10 - Elektronische Stimme P13 - Sensible Daten für den Verifier
Problembereich	Die Daten werden nach den Urnengang nicht (vollständig) vernichtet.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards löscht absichtlich / unabsichtlich nicht alle Daten, die vernichtet werden müssen.
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Weiterwendung der Daten

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
X	
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Vertraulichkeit der Daten wird nicht sichergestellt (Stimmgeheimnis).

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die Daten werden nicht oder nur teilweise gelöscht, was dazu führt, dass das Stimmgeheimnis langfristig gebrochen wird. Dies verursacht hohe Reputationsschäden.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**18**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers
			-

GEN-R04 - Daten werden nicht oder nur teilweise vernichtet und offengelegt (Post)

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Schutz der persönlichen Informationen über die Stimmberechtigten

Bedrohung

Informationsressourcen	P02 - Parameter des Urnengangs / Gegenstand des Urnengangs / Mitglieder Admin-Board und Electoral-Board / SRA-Templates von VOTING Stimmunterlagen / Verschlüsselungsparameter / Abstimmungs- und Wahloptionen (Primzahlen) P10 - Elektronische Stimme P13 - Sensible Daten für den Verifier
Problembereich	Die Daten werden nach den Urnengang nicht (vollständig) vernichtet.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
(2) Mittel Wie wird der Akteur vorgehen?	Die Post löscht absichtlich / unabsichtlich nicht alle Daten, die vernichtet werden müssen.
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Weiterwendung der Daten

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
X	
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Vertraulichkeit der Daten wird nicht sichergestellt (Stimmgeheimnis).

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die Daten werden nicht oder nur teilweise gelöscht, was dazu führt, dass das Stimmgeheimnis gebrochen wird. Dies verursacht hohe Reputationsschäden.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**18**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				Post

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

GEN-R05 - Änderung der Daten bei der Druckerei

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Bedrohung	**Informationsressourcen**	P09 - Stimmrechtsausweise (inkl. Stimmregister nicht anonymisiert, Codes)
	Problembereich	Durch veränderte Daten in der Druckerei können die Stimmberechtigen nicht abstimmen, oder die Gemeinden können die Doppelstimmprüfung nicht durchführen.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
	(2) Mittel Wie wird der Akteur vorgehen?	Es erfolgt eine Abstimmung zwischen einem Mitglied des Admin-Boards und einem Mitarbeiter der Druckerei, um Postscript-Dateien der SRAs zu bearbeiten. Es erfolgt eine Abstimmung zwischen einem Mitglied des Admin-Boards und einem Mitarbeiter der Druckerei, um das Register der Stimmrechtsausweise zu bearbeiten.
	(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch**: X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering**: X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Der elektronische Stimmkanal muss geschlossen werden. Die bereits abgegebenen elektronischen Stimmen werden nicht gezählt. Die Stimmberechtigten müssen physisch ihre Stimme abgeben. Es kann daher zu Beschwerden kommen, weil es Stimmberechtigte gibt, die nicht mehr genug Zeit für die Stimmabgabe haben. Zudem entsteht ein administrativer und kommunikativer Mehraufwand.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
Risiko-Score		**21**
Risiko-Stufe		**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Der Kanton hat die Prozesse gemeinsam mit der Druckerei definiert und in Checklisten festgehalten. Alle Schritte werden mittels 4-Augen-Prinzip durchgeführt. Die Datei mit den druckfertigen Stimmrechtsausweisen wird verschlüsselt (gemäss Anweisung der VEleS) und signiert übermittelt/übergeben. Die Prozesse der Druckerei wurden auditiert. Die Audits werden in regelmässigen Abständen wiederholt. Der Kanton hat zudem jederzeit das Recht, die Prozesse vor Ort zu beobachten.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
	X			Druckerei

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P01-R01 - Anpassung Informationswebseite

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Schutz der für die Stimmberechtigten bestimmten Informationen vor Manipulationen
Bedrohung	**Informationsressourcen**	P01 - Hilfsmittel für die Stimmberechtigten
	Problembereich	Anpassungen der Informationswebseite führen dazu, dass die Stimmberechtigten keinen Zugriff auf korrekte Informationen haben.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern
	(2) Mittel Wie wird der Akteur vorgehen?	Eine interne Person, die die Webseiten pflegt, begeht unabsichtlich einen Fehler, der die Datenänderung zur Folge hat. Ein interner Angreifer manipuliert die Informationswebsite bzw. das Abstimmungsportal und täuscht so die Stimmberechtigten. (LF 13.38)
	(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationsressourcen auf die Organisation oder den Inhaber?

Die Stimmberechtigten erhalten durch die Informationswebseite inkorrekte Informationen zur elektronischen Stimmabgabe. Aufgrund der inkorrekten Informationen gibt es mehr Supportanfragen, was zu einem erhöhten Supportaufwand führt.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**14**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Pflege der Webseiten kann nur durch berechtigten Personen durchgeführt werden.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P01-R02 - Die digitalen Erläuterungen stehen nicht mehr zur Verfügung

Risiko

Betroffene Kantone		GR
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		N/A
Bedrohung	**Informationsressourcen**	P01 - Hilfsmittel für die Stimmberechtigten
	Problembereich	Die Erläuterungen zu den Abstimmungsvorlagen werden digital vom Kanton bereitgestellt. Sie müssen den Stimmberechtigten während der Wahl- oder Abstimmungsphase zur Verfügung stehen.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	System
	(2) Mittel Wie wird der Akteur vorgehen?	Die Webseite des Kantons ist nicht mehr erreichbar und die digitalen Erläuterungen stehen nicht mehr zur Verfügung.
	(3) Motivation Warum tut er das?	N/A

(4) Ergebnis – Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
	X
Änderung	**Abbruch**

(5) Sicherheitsanforderungen – Warum wird die Sicherheitsanforderung nicht erfüllt?: Die Verfügbarkeit der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit – Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Ein Ausfall der Webseite würde den Zugang zu den Erläuterungen zum Zeitpunkt der Stimmabgabe verunmöglichen. Stimmberechtigte Personen können die Erläuterungen und Wahlanleitungen nicht zu Rate ziehen, was eine Einsprache nach sich ziehen könnte.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**16**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Webseite des Kantons Graubünden wird ständig überwacht. Ein Ausfall würde sofort bemerkt werden und die Störung könnte innert nützlicher Frist korrigiert werden.

Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers
		-	-

P01-R03 - Phishing / Spoofing durch E-Mail des Kantons

Risiko

Betroffene Kantone		GR
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Schutz der für die Stimmberechtigten bestimmten Informationen vor Manipulationen
Bedrohung	**Informationsressourcen**	P01 - Hilfsmittel für die Stimmberechtigten
	Problembereich	Die Stimmberechtigten können durch Phishing oder Spoofing beeinflusst werden (z.B. gefälschte Webseite).
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
	(2) Mittel Wie wird der Akteur vorgehen?	Da der Kanton per E-Mail mit den angemeldeten Stimmberechtigten kommuniziert, schickt ein Dritter E-Mails z.B. im Namen des Kantons, um die Stimmberechtigten zu beeinflussen (Pishing / Spoofing).
	(3) Motivation Warum tut er das?	Absichtlich: Manipulation des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Durch eine Spoofing-Mail werden die Stimmberechtigten des Kantons auf eine gefälschte Webseite geführt, die sie beispielsweise dazu bringt, die Codes einzugeben. Dadurch kennen die Angreifer die Codes und können anstelle der Stimmberechtigten abstimmen.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**14**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Information, ob die stimmberechtigte Person für E-Voting angemeldet ist sowie die entsprechende E-Mail-Adresse werden im Stimmregister der Gemeinden eingetragen und sind somit keine öffentlich zugänglichen Informationen. Eine breite Phishing/Spoofing-Kampagne kann erkannt werden.
Die Stimmberechtigten werden durch den Bestätigungsbrief im Rahmen des Anmeldeverfahrens auf die Sicherheitsinformationen zum Schutz vor Phishing-Mails aufmerksam gemacht.

Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers
		-	-

P02-R01 - Anpassung von Daten (Konfiguration/Stimmregister) stört den Urnengang

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Bedrohung	**Informationsressourcen**	P02 - Parameter des Urnengangs / Gegenstand des Urnengangs / Mitglieder Admin-Board und Electoral-Board / SRA-Templates von VOTING Stimmunterlagen / Verschlüsselungsparameter / Abstimmungs- und Wahloptionen (Primzahlen) P03 - EV-Stimmregister (nicht anonymisiert) P04 - EV-Stimmregister (anonymisiert)
	Problembereich	Die Daten für die Konfiguration des Urnengangs werden durch Interne/Externe/SW-Fehler angepasst, was zu eine Störung des Urnengangs führt.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern/Software
	(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards, welches für die Vorbereitung der Daten, den File-Import und dessen Integration in den SDM zuständig ist, begeht absichtlich/unabsichtlich einen Fehler, der eine Datenänderung zur Folge hat. Wegen eines Software-Fehlers im Ergebnisermittlungssystem werden fehlerhafte Urnengangsdaten für E-Voting bereitgestellt. Ein interner Angreifer nimmt eine fehlerhafte Konfiguration vor; es kommt nicht bis zur Auszählung. (LF 13.31)
	(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die für den Urnengang notwendigen Schritte können nicht durchgeführt werden, was bedeutet, dass die elektronische Stimmabgabe gestoppt werden muss. Die elektronischen Stimmen können nicht ausgezählt werden. Es kommt zu landesweiten Medienberichten.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**21**
	Risiko-Stufe	**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Alle Schritte werden mittels 4-Augen-Prinzip durchgeführt.
Durch Urnengangtests (E2E-Tests vor jedem Urnengang auf den produktiven Geräten) wird die Wahrscheinlichkeit des Risikos minimiert.
Die Konfiguration des Urnengangs wird während dem Prozess des Aufsetzens wiederholt im 4-Augen-Prinzip kontrolliert. Zu diesen Kontrollen gehört auch, dass am D1 nach der Erstellung der Stimmrechtsausweise anhand von Stichproben geprüft wird, ob die Codes bei der Generierung der Stimmrechtsausweise richtig übernommen wurden.
Am D2 wird jeweils anhand der Testurne geprüft, ob der Prozess bis und mit Entschlüsselung durchläuft. An der Konfiguration kann an D2 nichts mehr geändert werden. Die Wahrscheinlichkeit ist hoch, dass Probleme bei der Konfiguration rechtzeitig festgestellt würden. In einem solchen Fall müsste das Aufsetzen des Urnengangs wiederholt werden.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P02-R02 - Entnahme von sicherheitsrelevanten Daten

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Schutz der persönlichen Informationen über die Stimmberechtigten
Bedrohung	**Informationsressourcen**	P02 - Parameter des Urnengangs / Gegenstand des Urnengangs / Mitglieder Admin-Board und Electoral-Board / SRA-Templates von VOTING Stimmunterlagen / Verschlüsselungsparameter / Abstimmungs- und Wahloptionen (Primzahlen)
	Problembereich	Durch Entnahme sind sicherheitsrelevante Konfigurationsdaten nicht mehr vertraulich.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
	(2) Mittel Wie wird der Akteur vorgehen?	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. (LF 13.13)
	(3) Motivation Warum tut er das?	Absichtlich: Störung des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** X **Änderung** / **Abbruch**
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Vertraulichkeit der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Wenn bestimmte Informationen gestohlen werden, ist die Sicherheit des Urnengans (z.B. Stimmgeheimnis, Verifizierbarkeit) nicht mehr gewährleistet. Der elektronische Urnengang muss gestoppt werden, und zwar während der Wahl- oder Abstimmungsphase. Personen, die bereits abgestimmt haben, müssen erneut physisch abstimmen.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**20**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Daten befinden sich auf Offline-Geräten und auf Datenträgern, die in einem Safe (mittels 4-Augen-Prinzip) eingeschlossen werden.
Die Schritte werden mittels 4-Augen-Prinzip durchgeführt.
Der Virenscanner auf den Geräten wird vor jedem Urnengang aktualisiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P03-R01 - Offenlegung Stimmregister

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Schutz der persönlichen Informationen über die Stimmberechtigten

Bedrohung

Informationsressourcen	P03 - EV-Stimmregister (nicht anonymisiert) P18 - Register der Stimmrechtsausweise
Problembereich	Durch Offenlegung sind die im Stimmregister enthaltenen Daten nicht mehr vertraulich.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern
(2) Mittel Wie wird der Akteur vorgehen?	Ein interner Angreifer stiehlt Adressdaten der Stimmberechtigten. (LF 13.36) Ein Mitglied des Admin-Boards veröffentlicht das Register absichtlich/unabsichtlich. Ein Mitglied des Admin-Boards veröffentlicht das Register absichtlich/unabsichtlich. Ein Dritter kann durch Malware die Daten erhalten und veröffentlicht das Register.
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengang.

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
X	
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Vertraulichkeit der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Eine Offenlegung des Stimmregisters führt zu einem negativen, nationalen Medienecho.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**18**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Der Stimmregister verlässt die Offline-Geräte nicht.
Der Virenscanner auf den Geräten wird vor jedem Urnengang aktualisiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P04-R01 - Datenanpassung bei Anonymisierung des Stimmregisters

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Schutz der persönlichen Informationen über die Stimmberechtigten

Bedrohung

Informationsressourcen	P04 - EV-Stimmregister (anonymisiert)
Problembereich	Die anonymisierten Simmregisterdaten sind nicht deckungleich mit den Quelldaten.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Software
(2) Mittel Wie wird der Akteur vorgehen?	Wegen eines Software-Fehlers in der Software der Post (Configuration Computer) werden die Daten fehlerhaft anonymisiert.
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**
X	

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Durch eine Änderung der Daten gibt es Stimmberechtigte, die keine Möglichkeit haben, elektronisch abzustimmen. Sie können hingegen physisch abstimmen. Dies führt zu regionalen Medienberichten und zu mehr Support- und Kontrollaufwand.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**14**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch Urnengangtests (E2E-Tests vor jedem Urnengang) wird die Wahrscheinlichkeit des Risiko minimiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P04-R02 - Fehler bei Anonymisierung des Stimmregisters

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Schutz der persönlichen Informationen über die Stimmberechtigten

Bedrohung

Informationsressourcen	P03 - EV-Stimmregister (anonymisiert)
Problembereich	Durch eine fehlerhafte Anonymisierung werden Personendaten offengelegt.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Software
(2) Mittel Wie wird der Akteur vorgehen?	Wegen eines Software-Fehlers in der Software der Post (Configuration Computer) werden die Daten nicht korrekt anonymisiert.
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
X	
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Vertraulichkeit der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Bei der fehlerhaften Anonymisierung des Registers erhält die Post sensible Daten. Es folgt ein geringes Medienecho, da die Laien bereits davon ausgehen, dass die Post die Daten besitzt. Die DSG wird verletzt.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Tief	4
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**12**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch Urnengangtests (E2E-Tests vor jedem Urnengang) wird die Wahrscheinlichkeit des Risiko minimiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P07-R01 - Beide Passwörter sind einer Person bekannt

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse

Bedrohung

Informationsressourcen	P07 - Passwörter des Urnengangs
Problembereich	Die Passwörter werden angewendet, um die Privat-Schlüssel der Urnen zu generieren. Wenn die zwei Passwörter bei einer Person zusammenkommen, ist es möglich, die Urnen zu entschlüsseln.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards legt das Passwort absichtlich/unabsichtlich offen. Ein Mitglied des Electoral-Boards legt das Passwort absichtlich/unabsichtlich offen. Ein Mitglied des Admin-Boards kann sich die zwei Passwörter während des beobachteten Prozesses merken. Ein Mitglied des Electoral-Boards kann sich die zwei Passwörter während des beobachteten Prozesses merken.
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengangs

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
X	
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Passwörter müssen geheim bleiben und dürfen nie vor D3 zusammengefügt werden.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Wenn es möglich ist, die Stimmen vorzeitig zu lesen, wird das Vertrauen in E-Voting gefährdet.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**18**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Folgende Massnahmen wurden bereits getroffen:
- Die Passswörter werden mit einer genügenden Länge (mind. 50 Ziffern), mit Sonderzeichen und genügend Entropie generiert.
- Die zwei Passwörter werden separat aufbewahrt.
- Das Passwort des Admin-Boards wird im Safe aufbewahrt (4-Augen-Prinzip).
- Die Passwörter sind auf PIN-geschützen Datenträgern gespeichert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P07-R02 - Die Passwörter erlauben nicht, die Urnen zu entschlüsseln

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals

Bedrohung

Informationsressourcen	P07 - Passwörter des Urnengangs
Problembereich	Die Passwörter müssen wie im D2 definiert eingegeben werden. Sonst kann der Privat-Schlüssel nicht korrekt generiert werden und die Urnen können nicht enschlüsselt werden.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards ändert das Passwort absichtlich/unabsichtlich. Ein Mitglied des Admin-Boards vernichtet einen Datenträger mit dem Passwort absichtlich/unabsichtlich. Ein Mitglied des Electoral-Boards ändert das Passwort absichtlich/unabsichtlich. Ein Mitglied des Electoral-Boards vernichtet einen Datenträger mit dem Passwort absichtlich/unabsichtlich.
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengangs

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
X	
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Passwörter müssen geheim bleiben und dürfen nie vor D3 zusammengefügt werden.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Ohne die richtigen zwei Passwörter ist es nicht mehr möglich, die Urnen zu entschlüsseln. Die elektronischen Stimmen sind nicht auszählbar und können nicht berücksichtigt werden.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**21**
	Risiko-Stufe	**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Folgende Massnahmen wurden bereits getroffen:
- Die Passwörter werden je auf drei PIN-geschützen Datenträgern gespeichert.
- Die Generierung und Speicherung der Passwörter findet in einem beobachteten Prozess statt.
- Am D2 wird eine Testurne entschlüsselt, um sicherzustellen, dass der Prozess durchläuft.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P08-R01 - Offenlegung der Codes

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Korrektheit des Ergebnisses Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
Bedrohung	**Informationsressourcen**	P08 - Codes (Initialisierungs-, Bestätigungs- und Finalisierungscode sowie Prüfcodes) P09 - Stimmrechtsausweise (inkl. Stimmregister nicht anonymisiert, Codes)
	Problembereich	Mit den Codes kann ein Dritter für die Stimmberechtigten abstimmen Ein Dritter kann die Stimmabgabe von Wählenden manipulieren (Umgehung der individuellen und universellen Verifizierbarkeit, zB mit einer Schadsoftware auf der Plattform oder auf dem Server oder mit einem falschen Server)
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern
	(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards legt die Codes offen. Ein externer Angreifer erhält mittels Malware die Codes und legt diese offen. Ein interner Angreifer kopiert Stimmunterlagen und benutzt sie. (LF 13.11) Ein Mitglied der Admin-Boards verwendet den Datenträger unabsichtlich für einen anderen Zweck und dies führt zu einer Offenlegung. Ein externer Angreifer dringt elektronisch, physisch oder mittels Social Engineering in die Infrastruktur der Post ein und entwendet Stimmrechtsausweise. (LF 13.15)
	(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Manipulation des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** X **Änderung** / **Abbruch**
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Vertraulichkeit der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Der elektronische Stimmkanal muss geschlossen werden. Die bereits abgegebenen elektronischen Stimmen werden nicht gezählt. Die Stimmberechtigten müssen physisch ihre Stimme abgeben. Es kann daher zu Beschwerden kommen, weil es Stimmberechtigte gibt, die nicht mehr genug Zeit für die Stimmabgabe haben. Zudem entsteht ein administrativer und kommunikativer Mehraufwand. Es kann auch sein, dass der Angriff nur nach der Wahl oder gar nicht entdeckt wird. Die Wahl müsste dann wiederholt werden oder es würde ein nicht korrektes Ergebnis akzeptiert.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**21**
	Risiko-Stufe	**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Alle Schritte werden mittels 4-Augen-Prinzip durchgeführt.
Die Codes verlassen die Geräte nicht (ausser die Datei mit den druckfertigen Stimmrechtsausweisen). Die Geräte werden mittels 4-Augen-Prinzip aufbewahrt.
Die Datei mit den druckfertigen Stimmrechtsausweisen ist verschlüsselt und signiert (gemäss Anforderung der VEleS).
Die Mitarbeiter der Staatskanzlei unterstehen dem Amtsgeheimnis.
Die Plausibilisierung der Resultate könnte grössere Manipulationen aufdecken.
Die finanzielle Auswirkung bleibt tief, weil eine allfällige Wiederholung des Urnengangs an einem Blankoabstimmungstermin stattfinden wird.
Der Virenscanner auf den Geräten wird vor jedem Urnengang aktualisiert.
Zum Rechtlichen: Aufgrund der Erfahrungswerte der Kantone mit Beschwerden wurde die Kritikalität als "Mittel" eingestuft.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
	X			

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P08-R02 - Änderung der Codes

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Bedrohung	**Informationsressourcen**	P08 - Codes (Initialisierungs-, Bestätigungs- und Finalisierungscode sowie Prüfcodes) P09 - Stimmrechtsausweise (inkl. Stimmregister nicht anonymisiert, Codes)
	Problembereich	Ohne die richtigen Codes können die Stimmberechtigten ihre Stimme nicht abgeben / kontrollieren / bestätigen.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern/Software
	(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards verändert die Codes. Ein externer Angreifer verändert mittels Malware die Codes. Ein Mitglied des Admin-Boards verändert die Dateien unabsichtlich durch einen Handhabungsfehler. Es erfolgt eine Abstimmung zwischen einem Mitglied des Admin-Boards und einem Mitarbeiter der Druckerei, um Postscript-Dateien der SRAs zu bearbeiten. Ein Fehler in der Software zur Generierung der Stimmrechtsausweise verändert die Codes auf den SRAs.
	(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** | **Vernichtung / Verlust** **Änderung** | **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** | **Mittel** | **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Der elektronische Stimmkanal muss geschlossen werden. Die bereits abgegebenen elektronischen Stimmen werden nicht gezählt. Die Stimmberechtigten müssen physisch ihre Stimme abgeben. Es kann daher zu Beschwerden kommen, weil es Stimmberechtigte gibt, die nicht mehr genug Zeit für die Stimmabgabe haben. Zudem entsteht ein administrativer und kommunikativer Mehraufwand.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**21**
	Risiko-Stufe	**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Alle Schritte werden mittels 4-Augen-Prinzip durchgeführt.
Die Codes verlassen die Geräte nicht (ausser die Datei mit den druckfertigen Stimmrechtsausweisen). Die Geräte werden mittels 4-Augen-Prinzip aufbewahrt.
An D1 wird mittels Stichprobe kontrolliert, dass die Codes in den generierten PDFs (auf SRA Computer) mit den Codes in der Print-Datei (auf Configuration Computer) übereinstimmen. Am D2 wird mittels der Test- und Kontrollstimmen u.a. überprüft, ob die Codes übereinstimmen. Des Weiteren werden während des Abstimmungs- oder Wahlzeitraums regelmässig Teststimmen zur Kontrolle der Codes abgegeben.
Die Datei mit den druckfertigen Stimmrechtsausweisen ist verschlüsselt (gemäss Anweisung der VEleS) und signiert.
Die Mitarbeiter der Staatskanzlei unterstehen dem Amtsgeheimnis.
Der Virenscanner auf den Geräten wird vor jedem Urnengang aktualisiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
	X			

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P08-R03 - Änderung der Codes durch die Post

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals

Bedrohung

Informationsressourcen	P08 - Codes (Initialisierungs-, Bestätigungs- und Finalisierungscode sowie Prüfcodes)
Problembereich	Ohne die richtigen Codes können die Stimmberechtigten ihre Stimme nicht abgeben / kontrollieren / bestätigen.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern/Software
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitarbeiter der Post ändert die Dateien bevor die Übertragung an den Kanton erfolgt. Ein Softwarefehler verändert die Codes.
(3) Motivation Warum tut er das?	Absichtlich: Störung des Urnengangs Software: N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**
X	

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Der elektronische Stimmkanal muss geschlossen werden. Die bereits abgegebenen elektronischen Stimmen werden nicht gezählt. Die Stimmberechtigten müssen physisch ihre Stimme abgeben. Es kann daher zu Beschwerden kommen, weil es Stimmberechtigte gibt, die nicht mehr genug Zeit für die Stimmabgabe haben. Zudem entsteht ein administrativer und kommunikativer Mehraufwand.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**21**
	Risiko-Stufe	**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Konfiguration des Urnengangs wird mittels Verifier verifiziert. Bevor der Urnengang freigegeben wird, werden Test- und Kontrollstimmen abgegeben sowie Stichproben durchgeführt, um sicherzustellen, dass alles seine Richtigkeit hat (inkl. der Codes). Der Druck der Stimmrechtsausweise wird erst freigegen, wenn diese Prüfungen alle erfolgreich waren. Während des Abstimmungs- und Wahlzeitraums werden regelmässig Teststimmen zur Kontrolle der Codes abgegeben. Die korrekte Funktionsweise der Software wird durch die Kantone ausführlich getestet. Die Software ist offengelegt und es finden unabhängige Überprüfungen im Auftrag der Bundeskanzlei statt. Durch ein Trusted Build und Deployment wird sichergestellt, dass die richtige Software zum Einsatz kommt. Auch auf Seiten des Systemanbieters sind diverse Massnahmen umgesetzt, um die Wahrscheinlichkeit tief zu halten (insb. 4-Augen-Prinzip für den Zugriff auf die Infrastruktur). Die Prozesse bei der Post werden ebenfalls unabhängig überprüft.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
	X			Post

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P09-R01 - Offenlegung der SRAs in der Druckerei

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Korrektheit des Ergebnisses Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
Bedrohung	**Informationsressourcen**	P09 - Stimmrechtsausweise (inkl. Stimmregister nicht anonymisiert, Codes)
	Problembereich	Durch Zugang zu den Stimmrechtsausweise werden die Codes offengelegt, wodurch ein Dritter für die Stimmberechtigten abstimmen kann.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
	(2) Mittel Wie wird der Akteur vorgehen?	Die Druckerei wird von einem externen Hacker attackiert, die Daten werden gestohlen und veröffentlicht. Ein Mitarbeiter der Druckerei oder ein Kuvertierer legen die SRAs absichtlich / unabsichtlich offen. Ein externer Angreifer dringt elektronisch, physisch oder mittels Social Engineering in die Infrastruktur der Druckerei ein und entnimmt die Codes der Stimmrechtsausweise. (LF 13.14) Die SRAs werden während dem Transport zu Post offengelegt.
	(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Manipulation des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** X **Änderung** / **Abbruch**
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Vertraulichkeit der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Der elektronische Stimmkanal muss geschlossen werden. Die bereits abgegebenen elektronischen Stimmen werden nicht gezählt. Die Stimmberechtigten müssen physisch ihre Stimme abgeben. Es kann daher zu Beschwerden kommen, weil es Stimmberechtigte gibt, die nicht mehr genug Zeit für die Stimmabgabe haben. Zudem entsteht ein administrativer und kommunikativer Mehraufwand. es kann auch sein, dass der Angriff nur nach der Wahl oder gar nicht entdeckt wird. Die Wahl müsste dann wiederholt werden oder es würde ein nicht korrektes Ergebnis akzeptiert.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**21**
	Risiko-Stufe	**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Alle Schritte werden mittels 4-Augen-Prinzip durchgeführt.
Alle Schritte werden in Offline-Drucksystemen durchgeführt. Die Daten werden nur so lange aufbewahrt, wie absolut notwendig und werden anschliessend sicher gelöscht.
Die Plausibilisierung der Resultate könnte grössere Manipulationen aufdecken.
Die finanzielle Auswirkung bleibt tief, weil eine allfällige Wiederholung des Urnengangs an einem Blankoabstimmungstermin stattfinden wird.
Das Sicherheitsziel "Wahrung des Stimmgeheimnisses" ist betroffen, wenn ein Angreifer Zugang zum Stimmrechtsausweis sowie dem Gerät der stimmberechtigten Person hat und anhand der zurückgegebenen Codes erfährt, wie die stimmberechtigte Person abgestimmt hat.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
	X			Druckerei

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P09-R02 - Verzögerung bei Druck und Versand der SRAs

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals

Bedrohung

Informationsressourcen	P09 - Stimmrechtsausweise (inkl. Stimmregister nicht anonymisiert, Codes)
Problembereich	Ein Verlust der Daten auf den Datenträgern oder ein Problem bei der Druckerei führt dazu, dass einige Operationen wiederholt werden müssen.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern/Hardware
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boads vernichtet unabsichtlich einen Datenträger, was zum Verlust oder zur Vernichtung der Daten führt. Ein Mitglied des Admin-Boards verliert unabsichtlich den Datenträger mit SRAs beim Transport zwischen Staatskanzlei und Druckerei. Der Datenträger wird durch einen Mitarbeiter der Druckerei vernichtet, was zum Verlust oder zur Vernichtung der Daten führt. Der Datenträger kann bei der Druckerei nicht mehr gelesen werden. Die Kuvertiermaschine zerreisst SRAs.
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengangs

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
	X
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Verfügbarkeit der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die SRA müssen wieder aus dem Configuration Computer exportiert werden und erneut der Druckerei überbracht werden. Dies generiert Mehraufwand.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Tief	4
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**13**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P10-R01 - Verletzung des Stimmgeheimnisses

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse

Bedrohung

Informationsressourcen	P10 - Elektronische Stimme
Problembereich	Durch eine fehlerhafte Handhabung der Daten für die Prüfung oder durch Verwendung der Sicherheitsschlüssel des Urnengangs kann das Stimmgeheimnis gebrochen werden.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern
(2) Mittel Wie wird der Akteur vorgehen?	Bei der Prüfung auf Korrektheit der Verarbeitung und der Auszählung wird das Stimmgeheimnis gebrochen. (LF 13.24) Ein interner Angreifer benutzt den Schlüssel und entschlüsselt nicht-anonyme Stimmen. (LF 13.23)
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Stimmgeheimnis brechen

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	**Vernichtung / Verlust**
X	
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Vertraulichkeit der Daten wird nicht sichergestellt (Stimmgeheimnis).

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	**Mittel**	**Gering**
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Wenn das Stimmgehemnis gebrochen wird, löst dies landesweite Medienberichte aus.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
Risiko-Score		**18**
Risiko-Stufe		**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Stimmen sind gemäss dem kryptographischen Protokoll verschlüsselt.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	**Zu überwachen**	**Zu minimieren**	**Abgewälzt**	**Involvierte Dritte**
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P10-R02 - Stimmen werden an Dritte geschickt / von Dritten gelesen

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
Bedrohung	**Informationsressourcen**	P10 - Elektronische Stimme
	Problembereich	Durch eine Malware auf der Benutzerplattform kann das Stimmgeheimnis gebrochen werden.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
	(2) Mittel Wie wird der Akteur vorgehen?	Malware auf der Benutzerplattform schickt die Stimme an eine feindliche Organisation. (LF 13.20) Ein externer Angreifer liest die Stimme mittels MITM. (LF 13.22) Ein interner Angreifer manipuliert die Software und diese legt die Stimmen offen. (LF 13.28) Die Stimme wird mittels DNS-Spoofing umgeleitet. (LF 13.21)
	(3) Motivation Warum tut er das?	Absichtlich: Stimmgeheimnis brechen
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** | **Vernichtung / Verlust** X **Änderung** | **Abbruch**
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Vertraulichkeit der Daten wird nicht sichergestellt (Stimmgeheimnis).
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** | **Mittel** | **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Wenn das Stimmgehemnis gebrochen wird, löst dies landesweite Medienberichte aus.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
Risiko-Score		**18**
Risiko-Stufe		**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Stimmberechtigten werden an verschiedenen Stellen darauf hingewiesen, wie sie zur Sicherheit von E-Voting beitragen können (vgl. Konzept Information der Stimmberechtigten).

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P10-R03 - Veränderung der Stimmen zwischen den Geräten der Stimmberechtigten und Server

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Korrektheit des Ergebnisses

Bedrohung

Informationsressourcen	P10 - Elektronische Stimme
Problembereich	Die Stimme wird angepasst, bevor sie auf dem Server gespeichert wird.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
(2) Mittel Wie wird der Akteur vorgehen?	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). (13.6) Malware verändert die Stimme auf der Benutzerplattform. (LF 13.3) Ein externer Angreifer verändert die Stimme mit einer Man-in-the-middle-Technik (MITM -Technik). (LF 13.5) Ein externer Angreifer leitet die Stimme mittels Domain-Name-ServerSpoofing (DNS-Spoofing) um. (LF 13.4)
(3) Motivation Warum tut er das?	Absichtlich: Manipulation des Urnengangs

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**
X	

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Wenn die Stimme umgeleitet und/oder verändert wird, werden die Codes nicht richtig angezeigt. Dadurch sind die Prüfcodes nicht kontrollierbar und die betroffenen Stimmberechtigten müssen physisch abstimmen.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**19**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Stimmberechtigten werden an verschiedenen Stellen darauf darauf hingewiesen, wie sie zur Sicherheit von E-Voting beitragen können (vgl. Konzept Information der Stimmberechtigten). Dazu gehört beispielsweise die Kontrolle der Prüfcodes und die Prüfung der Hashwerte der Javascript-Dateien.
Durch die individuelle Verifizierbarkeit können mögliche Manipulation durch die stimmende Person erkannt werden.
Erläuterung zu Reputation und Vertrauen "hoch": Beispiel Demo DNS Spoofing System Genf löste nationale Berichterstattung aus und kann, wenn man es nicht schafft, dies richtig einzuordnen, das Vertrauen gefährden.
Hinweis: Dieses Risiko bzw. die Wirksamkeit der Massnahme ist mit P10-R06 verbunden.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P10-R04 - Manipulation der Stimmen innerhalb der Post

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Korrektheit des Ergebnisses

Bedrohung

Informationsressourcen	P10 - Elektronische Stimme
Problembereich	Die Stimme wird bei der Post verändert.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitarbeiter der Post verändert, löscht oder vervielfacht die Stimmen. Ein Mitarbeiter der Post löscht Stimmen. Eine feindliche Organisation dringt in das System ein mit dem Ziel, das Ergebnis zu fälschen. (LF 13.10) Ein interner Angreifer manipuliert die Software, diese speichert die Stimmen nicht. (13.7) Ein Mitarbeiter der Post fügt Stimmen ein.
(3) Motivation Warum tut er das?	Absichtlich: Manipulation des Urnengangs

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**
X	

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Wird die Stimme bei der Post verändert, wird dies durch die Mechanismen der universellen Verifizierbarkeit erkennbar. Die Reputation des Systemanbieters wird stark gefährdet und E-Voting wird gestoppt. Eine Beschwerde bezüglich der Korrektheit der Ergebnisse wird lanciert.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**21**
	Risiko-Stufe	**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch die universelle Verifizierbarkeit wird die Manipulation erkannt.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
	X			Post

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P10-R05 - Manipulation der Stimmen innerhalb des Kantons

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Korrektheit des Ergebnisses
Bedrohung	**Informationsressourcen**	P10 - Elektronische Stimme
	Problembereich	Durch eine interne Manipulation werden die Stimmen falsch auf dem Server gespeichert.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern
	(2) Mittel Wie wird der Akteur vorgehen?	Ein interner Angreifer verändert, löscht oder vervielfacht die Stimmen. (LF 13.8) Ein interner Angreifer fügt Stimmen ein. (LF 13.9)
	(3) Motivation Warum tut er das?	Absichtlich: Manipulation des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Wird die Stimme beim Kanton verändert, wird dies durch die Mechanismen der universellen Verifizierbarkeit erkennbar. Die Reputation des Kantons wird stark gefährdet und E-Voting wird gestoppt. Eine Beschwerde bezüglich der Korrektheit der Ergebnisse wird lanciert.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**20**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch die universelle Verifizierbarkeit wird die Manipulation erkannt.
Alle Schritte werden mittels 4-Augen-Prinzip und unter der Beobachtung der Prüferinnen und Prüfern durchgeführt.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P10-R06 - Codes werden von stimmberechtigten Personen nicht verifiziert

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Schutz der für die Stimmberechtigten bestimmten Informationen vor Manipulationen
Bedrohung	**Informationsressourcen**	P10 - Elektronische Stimme
	Problembereich	Ohne Verifikation der Codes durch die stimmberechtigten Personen, ist die individuelle Verifizierbarkeit nicht gegeben.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
	(2) Mittel Wie wird der Akteur vorgehen?	Ein externer Angreifer nutzt Social-Engineering-Methoden, um die Aufmerksamkeit der stimmenden Person an den Sicherheitsvorkehrungen vorbeizulenken (individuelle Verifizierbarkeit). (LF 13.12)
	(3) Motivation Warum tut er das?	Absichtlich: Manipulation des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** | **Vernichtung / Verlust** **Änderung** | **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** | **Mittel** | **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Ein Angreifer kann versuchen zu beweisen, dass die individuelle Verifizierbarkeit nicht funktioniert. Dies würde Medienberichte auslösen und das Vertrauen in E-Voting reduzieren.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
Risiko-Score		**18**
Risiko-Stufe		**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Informationen an die Stimmberechtigten erklären die Wichtigkeit der Prüfung.
Eine massive Attacke gegen die Benutzerplattform kann mit einem kleinen Anteil von vollständig geprüften Codes festgestellt werden (siehe z.B. https://moodlearchive.epfl.ch/2020-2021/pluginfile.php/2866714/mod_resource/content/1/mobileverification-ieee.pdf, Kapitel VI).

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P10-R07 - Stimmen können ohne Entschlüsselung gelesen werden

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse
Bedrohung	**Informationsressourcen**	P10 - Elektronische Stimme
	Problembereich	Durch ein Problem im Verschlüsselungsprozess wird das Stimmgeheimnis gebrochen.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern/Software
	(2) Mittel Wie wird der Akteur vorgehen?	Ein interner Angreifer liest die Stimmen vorzeitig, ohne die Stimmen entschlüsseln zu müssen. (LF 13.25) Ein Fehler im Verschlüsselungsprozess macht diesen funktionsunfähig oder reduziert seine Wirksamkeit. (LF 13.27) Eine feindliche Organisation dringt ins System ein mit dem Ziel, das Stimmgeheimnis zu brechen oder vorzeitige Teilergebnisse zu erheben. (LF 13.26)
	(3) Motivation Warum tut er das?	Absichtlich: Stimmgeheimnis brechen
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** X **Änderung** / **Abbruch**
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Vertraulichkeit der Daten wird nicht sichergestellt (Stimmgeheimnis).
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Wenn das System erlaubt, die Stimmen vorzeitig zu lesen, wird das Vertrauen in E-Voting gefährdet.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**18**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Stimmen sind gemäss dem kryptographischen Protokoll verschlüsselt.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P10-R08 - Anpassungen von Stimmen, ohne dass dies von der universellen Verifizierbarkeit bemerkt wird

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Korrektheit des Ergebnisses
Bedrohung	**Informationsressourcen**	P10 - Elektronische Stimme
	Problembereich	Die Wirkung der universellen Verifizierbarkeit ist zentral für das Vertrauen in den Urnengang.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Software
	(2) Mittel Wie wird der Akteur vorgehen?	Durch ein Problem mit der universellen Verifizierbarkeit werden die Stimmen angepasst, ohne, dass dies bemerkt wird (durch Bürger oder Electoral-Board).
	(3) Motivation Warum tut er das?	N/A
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?	**(8) Schwere** Wie schwer ist der Schaden je Risikobewertungskriterium?		
	Kriterium	**Kritikalität**	**Score**
Duch ein Problem mit der universellen Verifizierbarkeit werden Manipulationen nicht bemerkt. Dies führt zu fehlerhaften E-Voting Ergebnissen. Im Fall einer Bekanntmachung wird das Vertrauen in E-Voting langfristig sinken.	Reputation und Vertrauen	Hoch	12
	Finanzen	Tief	3
	Produktivität	Tief	1
	Gesundheit und Sicherheit	N/A	0
	Rechtliches	Mittel	4
	Andere	N/A	0
		Risiko-Score	**20**
		Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Das kryptographische Protokoll und die Implementierung wurde von der Bundekanzlei geprüft.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	**Zu überwachen**	**Zu minimieren**	**Abgewälzt**	**Involvierte Dritte**
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P10-R09 - Stimmen können nicht entschlüsselt werden

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals

Bedrohung

Informationsressourcen	P10 - Elektronische Stimme
Problembereich	Ohne Entschlüsselung (z.B. Problem mit der Kryptographie) ist es nicht möglich, die Stimmen auszuzählen.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Software
(2) Mittel Wie wird der Akteur vorgehen?	Durch einen Software-Fehler können die Stimmen nicht entschlüsselt werden.
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**
	X

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Verfügbarkeit der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die betroffenen elektronischen Stimmen können nicht ausgezählt und somit nicht berücksichtigt werden, was die Ergebnisse beeinflussen kann. Wenn der Einfluss auf die Ergebnisse hoch ist, muss der Urnengang wiederholt werden, was zu einem Mehraufwand führt.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**21**
	Risiko-Stufe	**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch Urnengangtests (E2E-Tests vor jedem Urnengang auf den produktiven Geräten) und die Abgabe und Entschlüsselung von Teststimmen am D2 wird die Wahrscheinlichkeit des Risikos minimiert.
Im Gegensatz zu GEN-R01, deckt dieses Risiko mehr Fälle ab als nur einen Computer-Ausfall.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
	X			

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P10-R10 - Fehler bei der individuellen Verifizierbarkeit

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Bedrohung	**Informationsressourcen**	P10 - Elektronische Stimme
	Problembereich	Die individuelle Verifizierbarkeit ist nicht mehr stichhaltig.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Software
	(2) Mittel Wie wird der Akteur vorgehen?	In der individuellen Verifizierbarkeit tritt ein Fehler auf. (LF 13.16)
	(3) Motivation Warum tut er das?	N/A
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Bei einem Fehler bei der individuellen Verifizierbarkeit können die Stimmberechtigten nicht mehr elektronisch abstimmen; sie müssen physisch abstimmen. Das Vertrauen in das System wird gefährdet, die Reputation von E-Voting wird reduziert, die Support- und Kontrallaufwände werden erhöht.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
Risiko-Score		**19**
Risiko-Stufe		**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch Urnengangtests (E2E-Tests vor jedem Urnengang) wird die Wahrscheinlichkeit des Risikos minimiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P10-R11 - Stimmenkauf durch Angreifer

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten
Bedrohung	**Informationsressourcen**	P10 - Elektronische Stimme
	Problembereich	Die Wahl- / Stimmfreiheit ist nicht gewährleistet.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern
	(2) Mittel Wie wird der Akteur vorgehen?	Ein interner Angreifer schreibt Stimmberechtigten vor, ob und wie sie abzustimmen oder zu wählen haben. Nach der Entschlüsselung findet er in der Infrastruktur Belege, dass sich die Stimmberechtigten an die Instruktionen gehalten haben. (LF 13.39) Ein externer Angreifer schreibt Stimmberechtigten vor, ob und wie sie abzustimmen oder zu wählen haben und verlangt von ihnen einen Beleg, dass sie sich an die Instruktionen gehalten haben. (LF 13.40)
	(3) Motivation Warum tut er das?	Absichtlich: Ergebnisse beeinflussen
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Bei einem bekanntgegebenen Stimmenkauf durch einen internen oder externer Angreifer wird die Reputation des Kantons und des elektronischen Stimmkanals reduziert.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
Risiko-Score		**14**
Risiko-Stufe		**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P10-R12 - Beinflussung der Meinungsbildung

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	keine missbräuchliche Verwendung von Beweisen zum Stimmverhalten

Bedrohung

Informationsressourcen	P10 - Elektronische Stimme
Problembereich	Die Stimme im System entspricht durch Beeinflussung nicht der intrinsischen Meinung des Stimmberechtigten.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
(2) Mittel Wie wird der Akteur vorgehen?	Malware beeinflusst stimmberechtigte Personen bei der Meinungsbildung. (LF 13.37)
(3) Motivation Warum tut er das?	Absichtlich: Ergebnisse beeinflussen

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**
X	

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Bei einer bekanntgegebenen Beeinflussung wird die Reputation des elektronischen Stimmkanals leicht reduziert und eine Beschwerde bezüglich der Korrektheit der Ergebnisse wird lanciert.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**20**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P10-R13 - Stimmabgabe ist durch Malware nicht möglich

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Bedrohung	**Informationsressourcen**	P10 - Elektronische Stimme
	Problembereich	Durch Malware können die Stimmberechtigen ihre elektronische Stimme nicht auf der Benutzerplattform abgeben.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
	(2) Mittel Wie wird der Akteur vorgehen?	Malware auf der Benutzerplattform macht die Stimmabgabe unmöglich. (LF 13.29)
	(3) Motivation Warum tut er das?	Absichtlich: Störung des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die elektronische Stimmabgabe ist nicht möglich; die Stimmberechtigen müssen physisch abstimmen. Die Reputation des elektronischen Stimmkanals wird reduziert.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**18**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Stimmberechtigten werden an verschiedenen Stellen darauf hingewiesen, wie sie zur Sicherheit von E-Voting beitragen können (vgl. Konzept Information der Stimmberechtigten).

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P11-R01 - Protokolle der Kontrollstimmen stehen nicht zur Verfügung

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals

Bedrohung

Informationsressourcen	P11 - Protokollierte Kontrollstimmen
Problembereich	Ohne die Protokolle der einzelnen Stimmen der Kontrollurne kann die Kontrolle am D3 nicht stattfinden.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitarbeiter der Staatskanzlei vernichtet unabsichtlich die Protokolle. Ein Mitarbeiter der Staatskanzlei stiehlt die Protokolle aus dem Tresor und vernichtet diese. Ein Dritter stiehlt die Protokolle aus dem Tresor und vernichtet diese.
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Verhinderung der Kontrolle

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
	X
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Verfügbarkeit der Daten (Protokolle) wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Da die Kontrolle nicht stattfinden kann, kann dieser Plausibilisierungsschritt nicht stattfinden und das Vertrauen in die Ergebnisse wird sinken.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**14**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Alle Schritte werden mittels 4-Augen-Prinzip durchgeführt.
Die Protokolle unterliegen dem 4-Augen-Prinzip.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P11-R02 - Protokolle der Kontrollstimmen stimmen mehrheitlich nicht mit den Ergebnissen überein

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Korrektheit des Ergebnisses

Bedrohung

Informationsressourcen	P11 - Protokollierte Kontrollstimmen
Problembereich	Die Protokolle der einzelnen Stimmen stimmen nicht mit den Ergebnissen der Kontrollurne überein.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitarbeiter der Staatskanzlei stiehlt die Protokolle aus dem Tresor und verändert diese. Ein Mitglied des Electoral-Boards protokolliert unabsichtlich / absichtlich falsch (nicht identisch mit dem, was im System abgestimmt wurde).
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Manipulation der Kontrolle

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**
X	

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die Plausibilisierung ist nicht korrekt und das Vertrauen in die Ergebnisse sinkt.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Tief	4
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**10**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Alle Schritte werden mittels 4-Augen-Prinzip durchgeführt.
Die Protokolle unterliegen dem 4-Augen-Prinzip.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P12-R01 - EV-Ergebnisse werden gelöscht, bevor sie ins Ergebnisermittlungssystem eingespielt werden

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals

Bedrohung

Informationsressourcen	P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen
Problembereich	Durch Löschung der Ergebnisse können diese nicht ausgezählt werden.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards löscht absichtlich / unabsichtlich die Datei mit den Ergebnissen.
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengangs

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
	X
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Verfügbarkeit der Daten wird nicht sichergestellt (EV-Ergebnisse stehen für die Auszählung nicht zur Verfügung).

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Wenn die Datei mit den Ergebnissen nicht mehr zur Verfügung steht, muss die Entschlüsselung erneut durchgeführt werden, was einen Mehraufwand und eine Verspätung der Publikation der Ergebnisse bedeutet.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Tief	4
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**11**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Alle Schritte werden mittels 4-Augen-Prinzip und unter der Beobachtung der Prüferinnen und Prüfern durchgeführt.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P12-R02 - Vorzeitige Offenlegung der EV-Ergebnisse

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Wahrung des Stimmgeheimnisses und Ausschluss vorzeitiger Teilergebnisse

Bedrohung

Informationsressourcen	P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen
Problembereich	Die Ergebnisse werden vor Abschluss der Abstimmungsphase offengelegt.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards legt die EV-Ergebnisse absichtlich / unabsichtlich offen, bevor der Urnengang abgeschlossen ist. Ein Mitglied des Electoral-Boards legt die EV-Ergebnisse absichtlich / unabsichtlich offen, bevor der Urnengang abgeschlossen ist.
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Politische Motivation

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
X	
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Vertraulichkeit der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Durch eine vorzeitige Offenlegung der EV-Ergebnisse werden die restlichen Stimmberechtigten, welche physisch abstimmen, beeinflusst. Dies liefert Grund für eine Beschwerde.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**14**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Alle in Wahlen und Abstimmungen involvierten Personen unterstehen dem Amtsgeheimnis.
Eine Entschlüsselung am Samstag erhöht die Auswirkung nicht. Die Wahrscheinlichkeit wird auch nicht erhöht. Die Kantone, die am Samstag entschlüsseln dürfen, zählen seit mehreren Jahren die brieflich abgegebenen Stimmen ebenfalls am Samstag aus, ohne, dass es je zu einem Vorfall bzw. einer frühzeitigen Offenlegung der Resultate kam. Die Prozesse sind eingespielt und die Verantwortlichkeiten klar.
Würden Resultate frühzeitig offengelegt, ist kaum zu erwarten, dass 1. eine Beeinflussung der Stimmberechtigten stattfinden und 2. dies einen Einfluss auf das Resultat hätte. Es gehen nur noch sehr wenige Leute an die Urne. Bei den Auslandschweizerinnen und Auslandschweizern kann ein Einfluss quasi ausgeschlossen werden. Sie haben nicht die Möglichkeit kurzfristig zu reagieren.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P12-R03 - EV-Ergebnisse werden geändert, bevor sie in Ergebnisermittlungssystem eingespielt werden

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Korrektheit des Ergebnisses
Bedrohung	**Informationsressourcen**	P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen
	Problembereich	Es werden fehlerhafte Ergebnisse publiziert.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern/Software
	(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards verändert absichtlich / unabsichtlich die Daten. Ein externer Angreifer verändert mittels Malware die EV-Ergebnisse, bevor diese in das Ergebnisermittlungssystem importiert werden. Durch einen Software-Fehler werden die Daten verändert in das Ergebnisermittlungssystem importiert.
	(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Da die Ergebnisse nicht übereinstimmen, muss untersucht werden, was passiert ist, und der Import in das Ergebnisermittlungssystem muss wiederholt werden.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Tief	4
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**11**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Alle Schritte werden mittels 4-Augen-Prinzip und unter der Beobachtung der Prüferinnen und Prüfern durchgeführt.
Die EV-Ergebnisse werden vom Electoral-Board im Ergebnisermittlungssysem geprüft.
Der Virenscanner auf den Geräten wird vor jedem Urnengang aktualisiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P12-R04 - EV-Ergebnisse werden nicht korrekt gezählt

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Korrektheit des Ergebnisses

Bedrohung

Informationsressourcen	P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen
Problembereich	Durch falsch ausgezählte Ergebnisse werden fehlerhafte Daten publiziert.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Software
(2) Mittel Wie wird der Akteur vorgehen?	Durch einen Software-Fehler werden die EV-Ergebnisse nicht korrekt gezählt.
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**
X	

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Es bedarf einer manuellen Auszählung aus eCH-0222, was einen Mehraufwand bedeutet. Die Ergebnisse müssen nachträglich angepasst werden. Dadurch ändern sich die konsolidierten Ergebnisse und es kommt zu regionalen Berichterstattungen.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**19**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch Urnengangtests (E2E-Tests vor jedem Urnengang) wird die Wahrscheinlichkeit des Risiko minimiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P13-R01 - Fehler oder Anomalie bei der Überprüfung der Ergebnisse

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Korrektheit des Ergebnisses
Bedrohung	**Informationsressourcen**	P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen P13 - Sensible Daten für den Verifier
	Problembereich	Der Verifier weist Fehler aus.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern/Software
	(2) Mittel Wie wird der Akteur vorgehen?	Ein technisches Hilfsmittel der Prüferinnen und Prüfer weist einen Fehler auf. (LF 13.18) Ein Mitglied des Admin-Boards verändert absichtlich / unabsichtlich die Daten. Ein Dritter kann durch eine Malware auf einem Gerät die Daten verändern. Ein interner Angreifer fälscht die kryptografischen Beweise der universellen Verifizierbarkeit. (LF 13.32) Ein Mitarbeiter der Post fälscht die kryptografischen Beweise der universellen Verifizierbarkeit. Ein Mitglied des Admin-Boards löscht absichtlich / unabsichtlich die Daten. Ein Dritter kann durch eine Malware auf einem Gerät die Daten löschen. Durch einen Fehler im Verifier können die Daten nicht gelesen werden.
	(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Manipulation des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	N/A
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die Überprüfung weist fatale Fehler oder Anomalien auf. Die EV-Ergebnisse können nicht berücksichtigt werden, da die Ursachen nicht rechtszeitig erforscht werden kann. Es kommt zu einem Reputationsschaden und zu einer Beschwerde betreffend der Ergebnisse.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**21**
	Risiko-Stufe	**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Es gibt einen Nottfall-Plan sowie eine Krisenvereinbarung.
Der Virenscanner auf den Geräten wird vor jedem Urnengang aktualisiert.
Im Rahmen der Urnengangtests (E2E-Tests vor jedem Urnengang) wird geprüft, ob der Verifier korrekt funktioniert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
	X			

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P13-R02 - Verifier kann nicht oder nur teilweise eingesetzt werden

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals

Bedrohung

Informationsressourcen	P12 - EV-Ergebnisse / Entschlüsselte elektronische Stimmen P13 - Sensible Daten für den Verifier
Problembereich	Die universelle Verifizierbarkeit ist nicht mehr stichhaltig.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Software
(2) Mittel Wie wird der Akteur vorgehen?	Ein technisches Hilfsmittel der Prüferinnen und Prüfer funktioniert zum Zeitpunkt der Auszählung nicht. (LF 13.34) In der universellen Verifizierbarkeit tritt ein Fehler auf. (LF 13.17) Durch einen Fehler im Verifier können die Daten nicht gelesen werden.
(3) Motivation Warum tut er das?	N/A

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**
	X

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Prüfung der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Der Urnengang kann nicht oder nur teilweise geprüft werden. Im Zweifelsfall werden die EV-Ergebnisse berücksichtigt und es werden anschliessend Nachforschungen angestellt, welche zu einer nachträglichen Korrektur der Ergebnisse führen können. Es kommt dadurch zu einem Mehraufwand.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**19**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch Urnengangtests (E2E-Tests vor jedem Urnengang) wird die Wahrscheinlichkeit des Risiko minimiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P14-R01 - Änderung der technischen Logs

Risiko

Betroffene Kantone	Alle	
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	
Bedrohung — **Informationsressourcen**	P14 - Ergebnisse des Verifiers / Papier-Protokolle / Technische Logs	
Problembereich	Durch Änderung oder Löschung der technischen Logs liefern die Untersuchungen falsche Ergebnisse.	
(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern	
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards verändert absichtlich / unabsichtlich die Logs. Ein Dritter kann durch Malware auf einem Gerät die Logs ändern. Ein Mitglied des Admin-Boards löscht absichtlich / unabsichtlich die Logs. Ein Dritter kann durch Malware auf einem Gerät die Logs löschen.	
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Manipulation verbergen	
(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung**	**Vernichtung / Verlust**
	Änderung	**Abbruch**
	X	
(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.	
(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch**	**Mittel** / **Gering**
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Durch Änderung/Löschung der technischen Logs können die Untersuchungen nicht sachgemäss durchgeführt werden, was Reputationsschäden verursacht.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
Risiko-Score		**20**
Risiko-Stufe		**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Der Virenscanner auf den Geräten wird vor jedem Urnengang aktualisiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P14-R02 - Änderung der technischen Logs bei der Post

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Bedrohung	**Informationsressourcen**	P14 - Ergebnisse des Verifiers / Papier-Protokolle / Technische Logs
	Problembereich	Durch Änderung oder Löschung der technischen Logs liefern die Untersuchungen falsche Ergebnisse.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
	(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitarbeiter der Post verändert absichtlich / unabsichtlich die Logs. Ein Dritter kann durch Malware die Logs bei der Post ändern. Ein Mitarbeiter der Post löscht absichtlich / unabsichtlich die Logs. Ein Dritter kann durch Malware die Logs bei der Post löschen.
	(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Manipulation verbergen
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Durch Änderung/Löschung der technischen Logs können die Untersuchungen nicht sachgemäss durchgeführt werden, was Reputationsschäden verursacht.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
Risiko-Score		**20**
Risiko-Stufe		**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Der Virenscanner auf den Geräten wird vor jedem Urnengang aktualisiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				**Post**

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P14-R03 - Fehlende Papier-Protokolle

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals

Bedrohung

Informationsressourcen	P14 - Ergebnisse des Verifiers / Papier-Protokolle / Technische Logs
Problembereich	Durch Löschung der Protokolle fehlt ein Mittel für allfällige Untersuchungen.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards vernichtet absichtlich / unabsichtlich die Papier-Protokolle. Ein Dritter vernichtet absichtlich die Papier-Protokolle.
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Untersuchungen verhindern

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
	X
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Verfügbarkeit der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Bei Untersuchungen müssen die Ereignisse durch eine Befragung der beteiligten Personen (insb. Electoral-Board) rekonstruiert werden, was zu Mehraufwand führt.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**16**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P15-R01 - Falsche Software installiert (Kanton)

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Bedrohung	**Informationsressourcen**	P15 - Software der Post beim Kanton (DIS, SDM, Verifier) P17 - Software von Abraxas beim Kanton (VOTING Stimmunterlagen; nur für SG)
	Problembereich	Mit der falschen Software wird den Urnengang nicht korrekt ablaufen oder anfällig für Manipulationen sein.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern
	(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards installiert absichtlich / unabsichtlich die falsche Software.
	(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung oder Manipulation des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** | **Vernichtung / Verlust** **Änderung** | **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** | **Mittel** | **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Einige Operationen können aufgrund der falschen Software nicht durchgeführt werden. Dadurch müssen Schritte wiederholt werden, was einen Mehraufwand bedeutet.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Tief	4
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
Risiko-Score		**11**
Risiko-Stufe		**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch Urnengangtests (E2E-Tests vor jedem Urnengang) und durch die Kontrolle der Hash-Werte wird die Wahrscheinlichkeit des Risiko minimiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P15-R02 - Manipulation von Software (Kanton)

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Bedrohung	**Informationsressourcen**	P15 - Software der Post beim Kanton (DIS, SDM, Verifier) P17 - Software von Abraxas beim Kanton (VOTING Stimmunterlagen; nur für SG)
	Problembereich	Durch die Manipulation von Software wird der Urnengang nicht korrekt ablaufen.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
	(2) Mittel Wie wird der Akteur vorgehen?	Eine Backdoor wird über eine Softwareabhängigkeit in das System eingeführt und von einem externen Angreifer ausgenutzt, um auf das System zuzugreifen. (LF 13.19) Ein Dritter verändert durch Malware die Software.
	(3) Motivation Warum tut er das?	Absichtlich: Störung oder Manipulation des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Einige Operationen können aufgrund der manipulierten Software nicht oder nur fehlerhaft durchgeführt werden (z.B. Schwächung kryptographischer Parameter). Dadurch müssen Schritte wiederholt werden, was einen Mehraufwand bedeutet.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
Risiko-Score		**19**
Risiko-Stufe		**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch Urnengangtests (E2E-Tests vor jedem Urnengang) und durch die Kontrolle der Hash-Werte wird die Wahrscheinlichkeit des Risikos minimiert.
Der Virenscanner auf den Geräten wird vor jedem Urnengang aktualisiert.
Der Verifier wird eingesetzt (während E2E-Tests und im Betrieb), um die kryptographischen Parameter zu prüfen.
Die Nichtoffenlegung der Software für die Erstellung der Stimmrechtsausweise (Nicht-Konformität) erhöht das Reputationskriterium auf "hoch".

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
		X		

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers
-	Die Kantone wollen die Nichtkonformität (Offenlegung der Software für die Erstellung der Stimmrechtsausweise) beheben. Sie planen, die nächste Version der Software VCPS zu veröffentlichen. Gemäss Planung dürfte dies im Verlauf von 2024 der Fall sein.	-	-

P16-R01 - Falsche Software installiert (Post)

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals

Bedrohung

Informationsressourcen	P16 - Software der Post bei der Post (E-Voting Server, Kontrollkomponenten, usw.)
Problembereich	Mit der falschen Software wird den Urnengang nicht korrekt ablaufen oder anfällig für Manipulationen sein.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitarbeiter der Post installiert absichtlich / unabsichtlich die falsche Software.
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung oder Manipulation des Urnengangs

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**
X	

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Einige Operationen können aufgrund der falschen Software nicht durchgeführt werden. Dadurch müssen Schritte wiederholt werden, was einen Mehraufwand bedeutet.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Tief	4
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**11**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Durch Urnengangtests (E2E-Tests vor jedem Urnengang) und Trusted Deployment wird die Wahrscheinlichkeit des Risiko minimiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				**Post**

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P16-R02 - Manipulation von Software (Post)

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Korrektheit des Ergebnisses

Bedrohung

Informationsressourcen	P16 - Software der Post bei der Post (E-Voting Server, Kontrollkomponenten, usw.)
Problembereich	Durch eine Manipulation der Software wird der Urnengang manipuliert.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
(2) Mittel Wie wird der Akteur vorgehen?	Ein Dritter kann durch Malware die Software verändern.
(3) Motivation Warum tut er das?	Absichtlich: Manipulation des Urnengangs

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
Änderung	**Abbruch**
X	

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Werden Stimmen durch die Manipulation von Software verändert, wird dies durch die Mechanismen der universellen Verifizierbarkeit erkennbar. Die Reputation des Systemanbieters wird stark gefährdet und E-Voting wird gestoppt.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
Risiko-Score		**20**
Risiko-Stufe		**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Mittels 4-Augen-Prinzip bei der Post wird die Wahrscheinlichkeit des Risikos minimiert.
Der Virenscanner auf den Geräten wird vor jedem Urnengang aktualisiert.
Der Verifier wird wahrscheinlich nicht betroffen sein. Die Software läuft nur bei den Kantonen. Die Kantone stellen sicher, dass sie die unveränderte Software im Einsatz haben.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P16-R03 - Nutzbare Schwachstellen in der Software der Post

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Korrektheit des Ergebnisses
Bedrohung	**Informationsressourcen**	P15 - Software der Post beim Kanton (DIS, SDM, Verifier) P16 - Software der Post bei der Post (E-Voting Server, Kontrollkomponenten, usw.)
	Problembereich	In der Software der Post existieren nutzbare Schwachstellen.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Extern
	(2) Mittel Wie wird der Akteur vorgehen?	Eine Backdoor wird über eine Softwareabhängigkeit in das System eingeführt und von einem externen Angreifer ausgenutzt, um auf das System zuzugreifen. (LF 13.19) Eine feindliche Organisation dringt ins System ein mit dem Ziel, den Betrieb zu stören, die Informationen für die Stimmberechtigten zu manipulieren oder Beweise zum Stimmverhalten der stimmenden Personen zu stehlen. (LF 13.35)
	(3) Motivation Warum tut er das?	Absichtlich: Manipulation des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität des Systems wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationsressourcen auf die Organisation oder den Inhaber?

Werden Stimmen durch die Schwachstellen in der Software verändert, wird dies durch die Mechanismen der universellen Verifizierbarkeit erkennbar. Die Reputation des Systemanbieters wird stark gefährdet und E-Voting wird gestoppt.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
	Risiko-Score	**20**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Mittels der Transparenzmassnahmen, Public Scrutiny sowie der unabhängigen Überprüfung im Auftrag der BK wird die Wahrscheinlichkeit des Risikos minimiert. Mittels Trusted Build und Trusted Deployment ist sichergestellt, dass die offengelegte Software eingesetzt wird.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				Post

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P18-R01 - Änderung des Registers der Stimmrechtsausweise

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Korrektheit des Ergebnisses
Bedrohung	**Informationsressourcen**	P18 - Register der Stimmrechtsausweise
	Problembereich	Ohne die richtige Verbindung zwischen dem Register der Stimmberechtigten und den Stimmrechtsausweisen könnte bei der Erstellung von Duplikaten Fehler auftreten.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern/Software
	(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied das Admin-Boards oder ein Mitarbeitender der Gemeinde ändert das Register absichtlich/unabsichtlich. Ein Dritter kann durch Malware das Register ändern. Durch einen Software-Fehler weist das Register Fehler auf. Es erfolgt eine Abstimmung zwischen einem Mitglied des Admin-Boards und einem Mitarbeiter der Druckerei, um Register zu bearbeiten.
	(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** **Änderung** / **Abbruch** X
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Integrität der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationsressourcen auf die Organisation oder den Inhaber?

Bei der Erstellung eines Duplikats wird der falsche Stimmrechtsausweis gesperrt. Eine Person kann folglich zweimal abstimmen und eine Person kann nicht mehr elektronisch abstimmen. Die Reputation von E-Voting sinkt.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Mittel	8
Finanzen	Tief	3
Produktivität	Tief	1
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**14**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Der Virenscanner auf den Geräten wird vor jedem Urnengang aktualisiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P19-R01 - Kompromittierte Signaturzertifikate

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Korrektheit des Ergebnisses
Bedrohung	**Informationsressourcen**	P19 - Signaturzertifikate
	Problembereich	Die Signaturzertifikate sind durch Anpassung oder Offenlegung kompromittiert und können nicht mehr verwendet werden. Die Kommunikationskanäle sind nicht mehr vertrauenswürdig.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern
	(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards legt die Privat-Schlüssel absichtlich/unabsichtlich offen. Ein Mitglied des Admin-Boards ändert die Privat-Schlüssel absichtlich/unabsichtlich. Ein Dritter kann durch Malware die Privat-Schlüssel einsehen und legt sie offen. Ein Dritter kann durch Malware die Privat-Schlüssel ändern.
	(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** | **Vernichtung / Verlust** X **Änderung** | **Abbruch**
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Verfügbarkeit der Daten wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** | **Mittel** | **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Die geänderten Zertifikate schwächen den Direct Trust, was die Manipulation des Transports erlaubt. Die Signaturzertifikate müssen ersetzt werden. Je nach Fortschritt kann dieses Ereignis Aufwände verursachen, indem gewisse Schritte wiederholt werden müssen.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Tief	4
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
Risiko-Score		**11**
Risiko-Stufe		**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Datei wird mittels 4-Augen-Prinzip angewendet und aufbewahrt.
Die Integrität und Authentizität der Zertifikat werden durch Fingerprints (Kontrolle durch physiches Meeting zwischen Herausgeber und Empfänger) geprüft, welche immer über einen separaten Kanal zur Verfügung gestellt werden.
Der Virenscanner auf den Geräten wird vor jedem Urnengang aktualisiert.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P20-R01 - Quorum des Admin-Boards kann nicht erreicht werden

Risiko

Betroffene Kantone		Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS		Erreichbarkeit und Funktionsfähigkeit des Stimmkanals
Bedrohung	**Informationsressourcen**	P20 - Passwörter des Admin-Boards (Profil)
	Problembereich	Ohne die Passwörter des Admin-Boards können die Aufgaben der Mitglieder des Admin-Boards (D1, D2 und D3) nicht durchgeführt werden. Insb. ist es nicht mehr möglich, die Urnen vorzubereiten oder zu entschlüsseln.
	(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern
	(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards vernichtet unabsichtlich/absichtlich die Kuverts mit den Passwörtern. Ein Mitglied des Admin-Boards vergisst sein Passwort.
	(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengangs
	(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?	**Offenlegung** / **Vernichtung / Verlust** X **Änderung** / **Abbruch**
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Verfügbarkeit der Daten für den Zugriff wird nicht sichergestellt.
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?	**Hoch** / **Mittel** / **Gering** X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Ohne Quorum (Admin-Board) ist es nicht mehr möglich, die Urne zu entschlüsseln. Die elektronischen Stimmen sind nicht auszählbar und können nicht berücksichtigt werden.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Hoch	12
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Mittel	4
Andere	N/A	0
Risiko-Score		**21**
Risiko-Stufe		**Signifikant**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Folgende Massnahmen wurden bereits getroffen:
- Nicht alle Mitglieder des Admin-Boards müssen anwesend sein. Das Quorum steht bei 2 Personen.
- Die Passwörter werden im Safe aufbewahrt, damit sie bei Abwesenheiten oder wenn jemand das Passwort vergessen hat, als Backup verfügbar sind.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
	X			

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers

P20-R02 - Die Passwörter sind offengelegt

Risiko

Betroffene Kantone	Alle
Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEleS	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals

Bedrohung

Informationsressourcen	P20 - Passwörter des Admin-Boards (Profil)
Problembereich	Das persönliche Passwort muss geheim bleiben, damit das 4-Augen-Prinzip gewährleistet ist.
(1) Akteur Wer wird die Bedrohung ausnutzen?	Intern/Extern
(2) Mittel Wie wird der Akteur vorgehen?	Ein Mitglied des Admin-Boards legt sein Passwort absichtlich/unabsichtlich offen. Eine externe Person stiehlt eine oder mehere Kuverts mit den Passwörtern.
(3) Motivation Warum tut er das?	Unabsichtlich: N/A Absichtlich: Störung des Urnengangs

(4) Ergebnis
Wie wirkt sich das auf die Informationssicherheit aus?

Offenlegung	Vernichtung / Verlust
X	
Änderung	**Abbruch**

(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?	Die Vertraulichkeit der Daten wird nicht sichergestellt.

(6) Wahrscheinlichkeit
Wie wahrscheinlich ist dieses Szenario?

Hoch	Mittel	Gering
		X

(7) Auswirkung
Welche Auswirkung (die schlimmste) haben die Informationressourcen auf die Organisation oder den Inhaber?

Alle Mitglieder kennen die Passwörter der anderen Mitglieder und das 4-Augen-Prinzip ist nicht mehr technisch gewährleistet. Es braucht zusätzliche Kontrollen, damit der Urnengang gemäss Prozess ablaufen kann.

(8) Schwere
Wie schwer ist der Schaden je Risikobewertungskriterium?

Kriterium	Kritikalität	Score
Reputation und Vertrauen	Tief	4
Finanzen	Tief	3
Produktivität	Mittel	2
Gesundheit und Sicherheit	N/A	0
Rechtliches	Tief	2
Andere	N/A	0
	Risiko-Score	**11**
	Risiko-Stufe	**Gering**

Erläuterungen
Weitere Erläuterungen/Bemerkungen zu der Beurteilung des Risikos

Die Passwörter kommen nur auf den Offline Computern zur Anwendung. Die Computer und Kuverts sind im Safe. Hier haben ebenfalls nur zwei Personen gemeinsam Zugriff. Ins Regierungsgebäude kommt man auch nicht ohne weiteres. Die Mitarbeitenden des Kantons sind vertrauenswürdig und werden im Umgang mit Passwörtern geschult. Es gibt Vorgaben zum Umgang mit Passwörtern.

(9) Risikobehandlung
Wie wird es aufgrund des Risikoscores gehandhabt?

Akzeptiert	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte
X				

Strategie zur Minimierung dieses Risikos (falls vorhanden):

Container, auf dem die Massnahme angewendet wird	Welche administrative, technische und physische Massnahme gilt für diesen Container?	Welches Restrisiko wird akzeptiert?	Abhängigkeit zu anderen Informationsressourcen und/oder Containers