



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 Umengang 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 Umengang nicht (vollständig) vernichtet.	P02 - Parameter des Umengangs / Gegenstand des Umengangs / 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 Umengang nicht (vollständig) vernichtet.	P02 - Parameter des Umengangs / Gegenstand des Umengangs / 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 Stimmberechtigten nicht abstimmen, oder die Gemeinden können die Doppeltstimmprüfung 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 Umengang	Alle	Erreichbarkeit und Funktionsfähigkeit des Stimmkanals	Die Daten für die Konfiguration des Umengangs werden durch Interne/Externe/SW-Fehler angepasst, was zu einer Störung des Umengangs führt.	P02 - Parameter des Umengangs / Gegenstand des Umengangs / 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 Umengangs / Gegenstand des Umengangs / Mitglieder Admin-Board und Electoral-Board / SRA-Templates von VOTING Stimmunterlagen / Verschlüsselungsparameter / Abstimmungs- und Wahloptionen (Primzahlen) P03 - EV-Stimmregister (nicht anonymisiert) P18 - Register der Stimmrechtsausweise	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 Stimmregisterdaten sind nicht deckungsgleich 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 Privatschlüssel der Urnen zu generieren. Wenn die zwei Passwörter bei einer Person zusammenkommen, ist es möglich, die Urnen zu entschlüsseln.	P07 - Passwörter des Umengangs	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 Privatschlüssel nicht korrekt generiert werden und die Urnen können nicht entschlüsselt werden.	P07 - Passwörter des Umengangs	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 Alle 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 Umengangs 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 Umengang.	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 auszuwählen.	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 - Beeinflussung 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 Stimmberechtigten 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 Ergebnismittlungssystem 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 Ergebnismittlungssystem 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 Umengang 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 Umengang 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 Umengang 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 Umgang 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.	P16 - 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 ungenügender Sicherheitsmassnahmen	Alle	N/A	Gegen einen Kanton wird Beschwerde eingereicht, weil er ein System betreibt 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 meist Stimmberichtigte für E-Voting an.	N/A	N/A	N/A	Gering	20	Gering	Akzeptiert	-

RPA-04 - Untersuchung eines Angriffs kann nicht ordentlich durchgeführt werden																																								
Risiko	Betroffene Kantone		Alle																																					
	Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VE/eS		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?		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">Offenlegung</td> <td style="width: 50%; text-align: center;">Vernichtung / Verlust</td> </tr> <tr> <td style="text-align: center;">Änderung</td> <td style="text-align: center;">Abbruch</td> </tr> </table>		Offenlegung	Vernichtung / Verlust	Änderung	Abbruch																															
		Offenlegung	Vernichtung / Verlust																																					
	Änderung	Abbruch																																						
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?		N/A																																					
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; text-align: center;">Hoch</td> <td style="width: 33%; text-align: center;">Mittel</td> <td style="width: 33%; text-align: center;">Gering</td> </tr> <tr> <td></td> <td></td> <td style="text-align: center;">X</td> </tr> </table>		Hoch	Mittel	Gering			X																														
	Hoch	Mittel	Gering																																					
			X																																					
	(7) Auswirkung Welche Auswirkung (die schlimmste) haben die Informationsressourcen auf die Organisation oder den Inhaber?		(8) Schwere Wie schwer ist der Schaden je Risikobewertungskriterium?																																					
Wenn die Untersuchungen nicht sachgemäss durchgeführt werden, verursacht dies Reputationsschäden.		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Kriterium</th> <th style="width: 20%;">Kritikalität</th> <th style="width: 20%;">Score</th> <th style="width: 30%;"></th> </tr> </thead> <tbody> <tr> <td>Reputation und Vertrauen</td> <td>Hoch</td> <td></td> <td style="text-align: right;">12</td> </tr> <tr> <td>Finanzen</td> <td>Tief</td> <td></td> <td style="text-align: right;">3</td> </tr> <tr> <td>Produktivität</td> <td>Tief</td> <td></td> <td style="text-align: right;">1</td> </tr> <tr> <td>Gesundheit und Sicherheit</td> <td>N/A</td> <td></td> <td style="text-align: right;">0</td> </tr> <tr> <td>Rechtliches</td> <td>Tief</td> <td></td> <td style="text-align: right;">2</td> </tr> <tr> <td>Andere</td> <td>N/A</td> <td></td> <td style="text-align: right;">0</td> </tr> <tr> <td colspan="3" style="text-align: right;">Risiko-Score</td> <td style="text-align: right;">18</td> </tr> <tr> <td colspan="3" style="text-align: right;">Risiko-Stufe</td> <td style="text-align: right;">Gering</td> </tr> </tbody> </table>			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
		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 Umrangings 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 X	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte																																				
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 VE/eS		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?		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">Offenlegung</td> <td style="width: 50%; text-align: center;">Vernichtung / Verlust</td> </tr> <tr> <td style="text-align: center;">Änderung</td> <td style="text-align: center;">Abbruch</td> </tr> </table>		Offenlegung	Vernichtung / Verlust	Änderung	Abbruch																															
		Offenlegung	Vernichtung / Verlust																																					
	Änderung	Abbruch																																						
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?		N/A																																					
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; text-align: center;">Hoch</td> <td style="width: 33%; text-align: center;">Mittel</td> <td style="width: 33%; text-align: center;">Gering</td> </tr> <tr> <td></td> <td></td> <td style="text-align: center;">X</td> </tr> </table>		Hoch	Mittel	Gering			X																														
	Hoch	Mittel	Gering																																					
			X																																					
	(7) Auswirkung Welche Auswirkung (die schlimmste) haben die Informationsressourcen auf die Organisation oder den Inhaber?		(8) Schwere Wie schwer ist der Schaden je Risikobewertungskriterium?																																					
Es könnte, je nach Auslöser, zu Reputationsschäden kommen (beispielsweise beim Fehlen von rechtlichen Grundlagen).		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Kriterium</th> <th style="width: 20%;">Kritikalität</th> <th style="width: 20%;">Score</th> <th style="width: 30%;"></th> </tr> </thead> <tbody> <tr> <td>Reputation und Vertrauen</td> <td>Mittel</td> <td></td> <td style="text-align: right;">8</td> </tr> <tr> <td>Finanzen</td> <td>Tief</td> <td></td> <td style="text-align: right;">3</td> </tr> <tr> <td>Produktivität</td> <td>Tief</td> <td></td> <td style="text-align: right;">1</td> </tr> <tr> <td>Gesundheit und Sicherheit</td> <td>N/A</td> <td></td> <td style="text-align: right;">0</td> </tr> <tr> <td>Rechtliches</td> <td>Tief</td> <td></td> <td style="text-align: right;">2</td> </tr> <tr> <td>Andere</td> <td>N/A</td> <td></td> <td style="text-align: right;">0</td> </tr> <tr> <td colspan="3" style="text-align: right;">Risiko-Score</td> <td style="text-align: right;">14</td> </tr> <tr> <td colspan="3" style="text-align: right;">Risiko-Stufe</td> <td style="text-align: right;">Gering</td> </tr> </tbody> </table>			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
		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?		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">Offenlegung</td> <td style="width: 50%; text-align: center;">Vernichtung / Verlust</td> </tr> <tr> <td style="text-align: center;">Änderung</td> <td style="text-align: center;">Abbruch</td> </tr> </table>		Offenlegung	Vernichtung / Verlust	Änderung	Abbruch																					
		Offenlegung	Vernichtung / Verlust																											
	Änderung	Abbruch																												
	(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?		N/A																											
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%; text-align: center;">Hoch</td> <td style="width: 33%; text-align: center;">Mittel</td> <td style="width: 33%; text-align: center;">Gering</td> </tr> <tr> <td></td> <td style="text-align: center;">X</td> <td></td> </tr> </table>		Hoch	Mittel	Gering		X																					
	Hoch	Mittel	Gering																											
		X																												
	(7) Auswirkung Welche Auswirkung (die schlimmste) haben die Informationsressourcen auf die Organisation oder den Inhaber? Das Vertrauen in die elektronische Stimmabgabe kann langfristig sinken.		(8) Schwere Wie schwer ist der Schaden je Risikobewertungskriterium? <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Kriterium</th> <th>Kritikalität</th> <th>Score</th> </tr> </thead> <tbody> <tr> <td>Reputation und Vertrauen</td> <td>Mittel</td> <td style="text-align: right;">8</td> </tr> <tr> <td>Finanzen</td> <td>Tief</td> <td style="text-align: right;">3</td> </tr> <tr> <td>Produktivität</td> <td>Tief</td> <td style="text-align: right;">1</td> </tr> <tr> <td>Gesundheit und Sicherheit</td> <td>N/A</td> <td style="text-align: right;">0</td> </tr> <tr> <td>Rechtliches</td> <td>Tief</td> <td style="text-align: right;">2</td> </tr> <tr> <td>Andere</td> <td>N/A</td> <td style="text-align: right;">0</td> </tr> <tr> <td colspan="2" style="text-align: right;">Risiko-Score</td> <td style="text-align: right;">14</td> </tr> <tr> <td colspan="2" style="text-align: right;">Risiko-Stufe</td> <td style="text-align: right;">Signifikant</td> </tr> </tbody> </table>		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	
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-12 - Ein Ausfall des Voter-Portals verhindert der Stimmabgabe																													
Risiko	Betroffene Kantone		GR																										
	Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VE/ESt		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?		<table border="1"> <tr> <td>Offenlegung</td> <td>Vernichtung / Verlust</td> </tr> <tr> <td>Änderung</td> <td>Abbruch</td> </tr> </table>		Offenlegung	Vernichtung / Verlust	Änderung	Abbruch																				
		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?		<table border="1"> <tr> <td>Hoch</td> <td>Mittel</td> <td>Gering</td> </tr> <tr> <td></td> <td></td> <td>X</td> </tr> </table>		Hoch	Mittel	Gering			X																			
	Hoch	Mittel	Gering																										
			X																										
	(7) Auswirkung Welche Auswirkung (die schlimmste) haben die Informationsressourcen auf die Organisation oder den Inhaber?		(8) Schwere Wie schwer ist der Schaden je Risikobewertungskriterium?																										
Ein Auslandschweizer / eine Auslandschweizerin reicht eine Beschwerde ein, weil er im Ausnahmefall (z.B. Total-Ausfall des E-Voting-Systems) nicht abstimmen kann.		<table border="1"> <thead> <tr> <th>Kriterium</th> <th>Kritikalität</th> <th>Score</th> </tr> </thead> <tbody> <tr> <td>Reputation und Vertrauen</td> <td>Mittel</td> <td>8</td> </tr> <tr> <td>Finanzen</td> <td>Tief</td> <td>3</td> </tr> <tr> <td>Produktivität</td> <td>Tief</td> <td>1</td> </tr> <tr> <td>Gesundheit und Sicherheit</td> <td>N/A</td> <td>0</td> </tr> <tr> <td>Rechtliches</td> <td>Mittel</td> <td>4</td> </tr> <tr> <td>Andere</td> <td>N/A</td> <td>0</td> </tr> <tr> <td colspan="2" style="text-align: right;">Risiko-Score</td> <td>16</td> </tr> <tr> <td colspan="2" style="text-align: right;">Risiko-Stufe</td> <td>Gering</td> </tr> </tbody> </table>	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
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 X	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte																									
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-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 VE/EoS		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 Auszahlung nicht verfügbar ist. (LF 13.33) Durch einer Naturkatastrophe 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?		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Offenlegung</th> <th style="width: 50%;">Vernichtung / Verlust</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Änderung</td> <td style="text-align: center;">Abbruch</td> </tr> <tr> <td></td> <td style="text-align: center;">X</td> </tr> </tbody> </table>		Offenlegung	Vernichtung / Verlust	Änderung	Abbruch		X																			
		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?		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 33%;">Hoch</th> <th style="width: 33%;">Mittel</th> <th style="width: 33%;">Gering</th> </tr> </thead> <tbody> <tr> <td></td> <td style="text-align: center;">X</td> <td></td> </tr> </tbody> </table>		Hoch	Mittel	Gering		X																					
	Hoch	Mittel	Gering																											
	X																													
(7) Auswirkung Welche Auswirkung (die schlimmste) haben die Informationssysteme auf die Organisation oder den Inhaber?		(8) Schwere Wie schwer ist der Schaden je Risikobewertungskriterium?																												
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.		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Kriterium</th> <th>Kritikalität</th> <th>Score</th> </tr> </thead> <tbody> <tr> <td>Reputation und Vertrauen</td> <td>Hoch</td> <td style="text-align: right;">12</td> </tr> <tr> <td>Finanzen</td> <td>Tief</td> <td style="text-align: right;">3</td> </tr> <tr> <td>Produktivität</td> <td>Tief</td> <td style="text-align: right;">1</td> </tr> <tr> <td>Gesundheit und Sicherheit</td> <td>N/A</td> <td style="text-align: right;">0</td> </tr> <tr> <td>Rechtliches</td> <td>Mittel</td> <td style="text-align: right;">4</td> </tr> <tr> <td>Andere</td> <td>N/A</td> <td style="text-align: right;">0</td> </tr> <tr> <td colspan="2" style="text-align: right;">Risiko-Score</td> <td style="text-align: right;">20</td> </tr> <tr> <td colspan="2" style="text-align: right;">Risiko-Stufe</td> <td style="text-align: right;">Signifikant</td> </tr> </tbody> </table>		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
		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																														
<p>Durch Releasetests sowie Urnengangstests (E2E-Tests vor jedem Urnengang auf den produktiven Geräten) wird die Wahrscheinlichkeit des Risikos minimiert. Sowohl die Post (Splunk-Reporting und Überwachung der Infrastruktur) 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.</p> <p>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.</p> <p>Die Kantone haben mit der Post ein SLA abgeschlossen, welches die Reaktions- 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.</p> <p>Graubünden: Ein Total-Ausfall des Systems während des Abstimmungs- oder Wahlzeitraums ist zusätzlich im Risiko RPA-12 adressiert.</p>																														
(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																													

P01-R02 - Die digitalen Erläuterungen stehen nicht mehr zur Verfügung												
Risiko	Betroffene Kantone		GR									
	Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VEieS		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?		<table border="1"> <tr> <td>Offenlegung</td> <td>Vernichtung / Verlust</td> </tr> <tr> <td></td> <td>X</td> </tr> <tr> <td>Änderung</td> <td>Abbruch</td> </tr> <tr> <td></td> <td></td> </tr> </table>	Offenlegung	Vernichtung / Verlust		X	Änderung	Abbruch		
		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?		<table border="1"> <tr> <td>Hoch</td> <td>Mittel</td> <td>Gering</td> </tr> <tr> <td></td> <td></td> <td>X</td> </tr> </table>	Hoch	Mittel	Gering			X			
Hoch	Mittel	Gering										
		X										
(7) Auswirkung Welche Auswirkung (die schlimmste) haben die Informationsressourcen auf die Organisation oder den Inhaber?		(8) Schwere Wie schwer ist der Schaden je Risikobewertungskriterium?										
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.		Kriterium	Kritikalität									
		Reputation und Vertrauen	Mittel									
		Finanzen	Tief									
		Produktivität	Tief									
		Gesundheit und Sicherheit	N/A									
		Rechtliches	Mittel									
		Andere	N/A									
		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 X	Zu überwachen	Zu minimieren	Involvierte Dritte									
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 VEieS		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 (Phishing / Spoofing).																									
		(3) Motivation Warum tut er das?		Absichtlich: Manipulation des Urnengangs																									
		(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?		<table border="1"> <thead> <tr> <th>Offenlegung</th> <th>Vernichtung / Verlust</th> </tr> </thead> <tbody> <tr> <td>Änderung</td> <td>Abbruch</td> </tr> <tr> <td>X</td> <td></td> </tr> </tbody> </table>	Offenlegung	Vernichtung / Verlust	Änderung	Abbruch	X																				
		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?		<table border="1"> <thead> <tr> <th>Hoch</th> <th>Mittel</th> <th>Gering</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td>X</td> </tr> </tbody> </table>	Hoch	Mittel	Gering			X																				
	Hoch	Mittel	Gering																										
		X																											
(7) Auswirkung Welche Auswirkung (die schlimmste) haben die Informationsressourcen auf die Organisation oder den Inhaber?		(8) Schwere Wie schwer ist der Schaden je Risikobewertungskriterium?																											
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.		<table border="1"> <thead> <tr> <th>Kriterium</th> <th>Kritikalität</th> <th>Score</th> </tr> </thead> <tbody> <tr> <td>Reputation und Vertrauen</td> <td>Mittel</td> <td>8</td> </tr> <tr> <td>Finanzen</td> <td>Tief</td> <td>3</td> </tr> <tr> <td>Produktivität</td> <td>Tief</td> <td>1</td> </tr> <tr> <td>Gesundheit und Sicherheit</td> <td>N/A</td> <td>0</td> </tr> <tr> <td>Rechtliches</td> <td>Tief</td> <td>2</td> </tr> <tr> <td>Andere</td> <td>N/A</td> <td>0</td> </tr> <tr> <td colspan="2" style="text-align: right;">Risiko-Score</td> <td>14</td> </tr> <tr> <td colspan="2" style="text-align: right;">Risiko-Stufe</td> <td>Gering</td> </tr> </tbody> </table>	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
		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 X	Zu überwachen	Zu minimieren	Abgewälzt																										
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 VE/ESt		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	
		(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?		X	Abbruch	
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?					
	(7) Auswirkung Welche Auswirkung (die schlimmste) haben die Informationsressourcen auf die Organisation oder den Inhaber?		(8) Schwere Wie schwer ist der Schaden je Risikobewertungskriterium?			
	Wenn bestimmte Informationen gestohlen werden, ist die Sicherheit des Urnengangs (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.		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 Virens Scanner 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				

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 VE/eS		Korrektheit des Ergebnisses																												
	Bedrohung	Informationsressourcen		P10 - Elektronische Stimme																											
		Problemereich		Die Wirkung der universellen Verifizierbarkeit ist zentral für das Vertrauen in den Urnengang.																											
		(1) Akteur Wer wird die Bedrohung ausnutzen?		Software																											
		(2) Mittel <small>(SICHERHEIT, VERTRAUEN, VERBODEN, VERGEBEN)</small>		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?		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">Offenlegung</td> <td style="text-align: center;">Vernichtung / Verlust</td> </tr> <tr> <td style="text-align: center;">Änderung</td> <td style="text-align: center;">Abbruch</td> </tr> <tr> <td style="text-align: center;">X</td> <td></td> </tr> </table>		Offenlegung	Vernichtung / Verlust	Änderung	Abbruch	X																					
		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?		<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">Hoch</td> <td style="text-align: center;">Mittel</td> <td style="text-align: center;">Gering</td> </tr> <tr> <td></td> <td></td> <td style="text-align: center;">X</td> </tr> </table>		Hoch	Mittel	Gering			X																					
	Hoch	Mittel	Gering																												
			X																												
(7) Auswirkung Welche Auswirkung (die schlimmste) haben die Informationssysteme auf die Organisation oder den Inhaber?		(8) Schwere Wie schwer ist der Schaden je Risikobewertungskriterium?																													
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.		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Kriterium</th> <th>Kritikalität</th> <th>Score</th> </tr> </thead> <tbody> <tr> <td>Reputation und Vertrauen</td> <td>Hoch</td> <td style="text-align: right;">12</td> </tr> <tr> <td>Finanzen</td> <td>Tief</td> <td style="text-align: right;">3</td> </tr> <tr> <td>Produktivität</td> <td>Tief</td> <td style="text-align: right;">1</td> </tr> <tr> <td>Gesundheit und Sicherheit</td> <td>N/A</td> <td style="text-align: right;">0</td> </tr> <tr> <td>Rechtliches</td> <td>Mittel</td> <td style="text-align: right;">4</td> </tr> <tr> <td>Andere</td> <td>N/A</td> <td style="text-align: right;">0</td> </tr> <tr> <td colspan="2" style="text-align: right;">Risiko-Score</td> <td style="text-align: right;">20</td> </tr> <tr> <td colspan="2" style="text-align: right;">Risiko-Stufe</td> <td style="text-align: right;">Gering</td> </tr> </tbody> </table>			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
		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																															
Das kryptographische Protokoll und die Implementierung wurde von der Bundeskanzlei geprüft.																															
(9) Risikobehandlung																															
Wie wird es aufgrund des Risikoscores gehandhabt?																															
Akzeptiert X	Zu überwachen	Zu minimieren	Abgewälzt	Involvierte Dritte																											
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 Urngangs		
		(4) Ergebnis Wie wirkt sich das auf die Informationssicherheit aus?		Offenlegung	Vernichtung / Verlust	
		(5) Sicherheitsanforderungen Warum wird die Sicherheitsanforderung nicht erfüllt?		Änderung	Abbruch	
	(6) Wahrscheinlichkeit Wie wahrscheinlich ist dieses Szenario?		X			
	(7) Auswirkung Welche Auswirkung (die schlimmste) haben die Informationsressourcen auf die Organisation oder den Inhaber?		(8) Schwere Wie schwer ist der Schaden je Risikobewertungskriterium?			
	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.		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 Virens Scanner 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.	-	-			

P20-R01 - Quorum des Admin-Boards kann nicht erreicht werden																															
Risiko	Betroffene Kantone		Alle																												
	Sicherheitsziel(e) Gemäss Art. 4 Ziff. 3 VE/ESt		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?		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Offenlegung</th> <th style="width: 50%;">Vernichtung / Verlust</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Änderung</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">Abbruch</td> <td style="text-align: center;">Abbruch</td> </tr> </tbody> </table>		Offenlegung	Vernichtung / Verlust	Änderung	X	Abbruch	Abbruch																				
		Offenlegung	Vernichtung / Verlust																												
	Änderung	X																													
	Abbruch	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?		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 33%;">Hoch</th> <th style="width: 33%;">Mittel</th> <th style="width: 33%;">Gering</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td style="text-align: center;">X</td> </tr> </tbody> </table>		Hoch	Mittel	Gering			X																					
	Hoch	Mittel	Gering																												
		X																													
(7) Auswirkung Welche Auswirkung (die schlimmste) haben die Informationsressourcen auf die Organisation oder den Inhaber?		(8) Schwere Wie schwer ist der Schaden je Risikobewertungskriterium?																													
Ohne Quorum (Admin-Board) ist es nicht mehr möglich, die Urne zu entschlüsseln. Die elektronischen Stimmen sind nicht auszählbar und können nicht berücksichtigt werden.		<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Kriterium</th> <th style="width: 20%;">Kritikalität</th> <th style="width: 50%;">Score</th> </tr> </thead> <tbody> <tr> <td>Reputation und Vertrauen</td> <td>Hoch</td> <td style="text-align: right;">12</td> </tr> <tr> <td>Finanzen</td> <td>Tief</td> <td style="text-align: right;">3</td> </tr> <tr> <td>Produktivität</td> <td>Mittel</td> <td style="text-align: right;">2</td> </tr> <tr> <td>Gesundheit und Sicherheit</td> <td>N/A</td> <td style="text-align: right;">0</td> </tr> <tr> <td>Rechtliches</td> <td>Mittel</td> <td style="text-align: right;">4</td> </tr> <tr> <td>Andere</td> <td>N/A</td> <td style="text-align: right;">0</td> </tr> <tr> <td colspan="2" style="text-align: right;">Risiko-Score</td> <td style="text-align: right;">21</td> </tr> <tr> <td colspan="2" style="text-align: right;">Risiko-Stufe</td> <td style="text-align: right;">Signifikant</td> </tr> </tbody> </table>			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
		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																													

