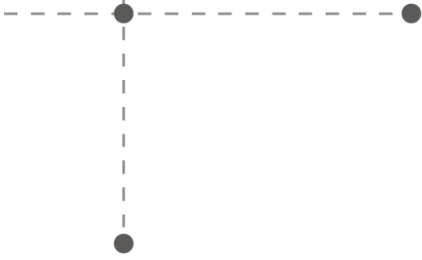




Cyberdefense



Federal Chancellery

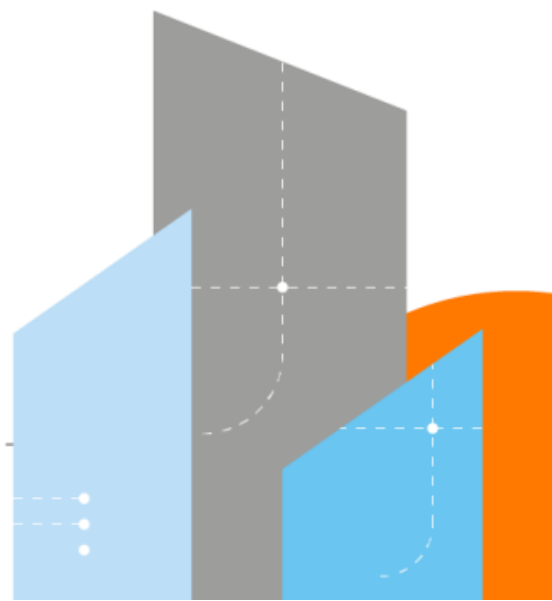
Examination of the Swiss Internet voting system

**Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures
of the canton**

9 January 2026



Orange Restricted



Contact information

Address	Contact
Orange Cyberdefense Switzerland SA Rue du Sablon 4 1110 Morges	Stéphane Adamiste Chief Product Officer +41 21 802 64 01 stephane.adamiste@orange cyberdefense.com

Contributors

Name	Role
Stéphane Adamiste	Chief Product Officer, Orange Cyberdefense Switzerland

Document history

Version	Date	Author	Change details
0.1	26 November 2025	Stéphane Adamiste	Working version
0.9	23 December 2025	Stéphane Adamiste	Draft for review
1.0	09 January 2026	Stéphane Adamiste	Released version

Contents

1	Context	5
2	Methodology	7
2.1	Process	7
2.2	Collection of evidence	7
2.3	Findings	7
2.4	Classification of findings	7
2.5	Relevance of the assessment criteria	8
2.6	Assumptions	8
3	Impact analysis of release 1.5	9
4	Assessment results	13
5	Summary of findings and recommendations	23
6	References	24

Management summary

Context, scope and objective of the examination

This examination work was mandated by the Federal Chancellery following a major release (i.e., R1.5) of the e-voting application by Swiss Post.

The objective of the examination was to assess to which extent the introduction of the new software version affects the overall compliance level of the cantons of Basel-Stadt, Graubünden, St. Gallen and Thurgau with the applicable requirements of the Ordinance on Electronic Voting (“VEleS”, or “OEV”), audit scope *3c) Assess the infrastructure and organisational measures of the canton.*

Unlike the previous audit conducted in 2024 for the R1.4 release, during which all criteria of scope *3c* were assessed, the examiners defined the scope at their discretion, focusing specifically on the requirements that could be affected by the new software release. A subset of twenty-seven (27) OEV requirements was selected to form the audit scope.

Methodology

The examiners analysed the release note published by Swiss Post for versions 1.5 and identified the OEV requirements potentially affected by the new release. They then sought evidence of compliance with these requirements through the review of relevant documentation (e.g. policies, procedures, specifications, reports, processes).

Results

Overall, the cantons have demonstrated a high level of compliance with the applicable OEV requirements of the ordinance on e-voting: One potential improvement was identified.

Recommendation

The examiners suggest that the cantons document the impact of the improvements introduced by the 1.5 version of the e-voting software on the likelihood of the related risks in their portfolio.

Final note

The examiners conclude this summary by thanking the cantons of Basel Stadt, Graubünden, St. Gallen and Thurgau for their cooperation and for the transparency demonstrated throughout the examination.

1 Context

1. Electronic voting (hereafter referred to as: “e-voting”) was introduced in Switzerland through multiple pilot schemes from 2004 onwards. A total of 15 cantons made e-voting possible in over 300 trials, until early 2019. Two implementations were available: the system provided by the canton of Geneva and the system operated by the Swiss Post (hereafter also referred to as “the Post”), initially developed by ScytL. In June 2019, the canton of Geneva announced the withdrawal of its e-voting system with immediate effect. It was followed in July of the same year by the announcement by the Swiss Post of the withdrawal of its e-voting system from operation to focus on improving the solution. At that point, e-voting was no longer possible in Switzerland.
2. In June 2019, the Swiss Federal Chancellery (hereafter also referred to as “Federal Chancellery”) was commissioned by the Federal Council to redesign a new trial phase, in collaboration with the cantons, using “e-voting systems, which are fully verifiable” [1]. This redesign of the trial phase focused on four objectives:
 - a) Further development of the e-voting systems
 - b) Effective controls and monitoring
 - c) Increased transparency and trust
 - d) Stronger connection with the scientific community
3. A taskforce was set up to make proposals for the future of internet voting. To that end, the Federal Chancellery invited experts from academia and industry to engage in a broad dialogue on internet voting in Switzerland. After this dialog, the Federal Chancellery and the cantons published a final report on the redesign and relaunch of internet voting trials, with a catalogue of measures [2].
4. The Federal Council took note of the final report and commissioned the Federal Chancellery to amend the legal bases of the Confederation regarding e-voting. In April 2021, the Federal Council opened a consultation procedure for the redesign of the e-voting trials. The redesign includes both a partial revision of the Ordinance on Political Rights (PoRo) [3] and a complete revision of the Federal Chancellery Ordinance on Electronic Voting (“VEleS”, or “OEV”) [4]. The OEV specifies, among others, the requirements for authorising electronic voting, including the technical and administrative controls for approving an e-voting system.
5. The Federal Chancellery issued an audit concept for the examination of Swiss internet voting systems defining the foundations for assessing the compliance of electronic voting systems with the draft OEV and its annex, as per chapter 26 of the annex of the draft OEV, and for obtaining recommendations for improvements [5].
6. In May 2022, the Federal Council enacted the partially revised Ordinance on Political Rights (PoRo) [6], which became applicable from July 1st 2022. The totally revised Federal Chancellery Ordinance on Electronic Voting (OEV) [7] came into force on the same date.

7. In September 2022, an updated version of the audit concept was issued by the Federal Chancellery [8].
8. Orange Cyberdefense Switzerland (“OCD CH”, formerly SCRT) was mandated by the Federal Chancellery to assess the compliance of the cantons planning to use the revamped e-voting system provided by the Post against the requirements of the OEV applicable to cantons. The concerned cantons are: Basel-Stadt, St. Gallen, Thurgau and Graubünden.
9. At its meeting on 16 August 2023, the Federal Council granted the cantons of Basel-Stadt, St. Gallen and Thurgau basic licences to trial online voting (e-voting) in the National Council elections on 22 October 2023 [9]
10. At its meeting on 22 November 2023, the Federal Council granted the canton of Graubünden a basic licence for trials with electronic voting in federal votes. [10]
11. Following the release of a new version of the Post’s e-voting system (v1.4), OCD CH has been requested to update its audit work [11], [12] concerning the cantons in 2024. The objective was to analyse the potential implications that the release of version 1.4 might have on the compliance of the cantons' practices with the requirements of the OEV.
12. In 2025, OCD CH was once again mandated by the Federal Chancellery to perform a new, full-scope audit of the e-voting system provided by the Post. On this occasion, the Federal Chancellery updated its audit concept to include additional requirements [13].
13. Following the release of version 1.5 of the software, an additional assessment was carried out to analyse the potential implications on the compliance level of Basel-Stadt, Graubünden, St. Gallen and Thurgau.

2 Methodology

2.1 Process

14. The examination was based on OCD CH's information systems audit methodology. The process specifies four-phases, as depicted in the figure below:

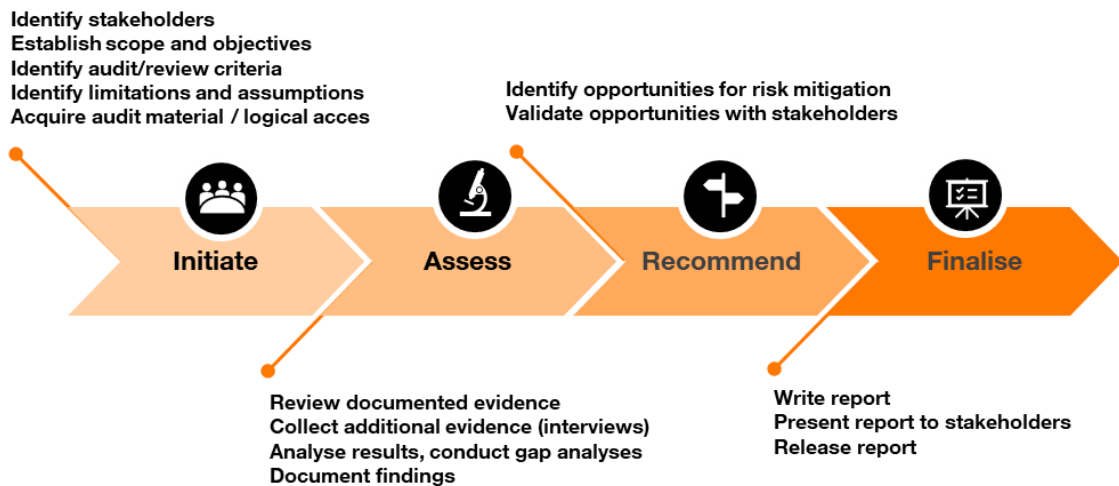


Figure 1: Examination process

2.2 Collection of evidence

15. As a general principle, the examiners aimed at acquiring two types of evidence for each requirement. Types of evidence included: documents (e.g., policies, procedures, reports, etc.) and statements obtained from examinees during interviews.

2.3 Findings

16. The examiners raised a finding when evidence provided by the examinee did not provide satisfying assurance that the requirement is met (implicit miss) or when evidence provided explicitly indicates that the requirement is not or partially satisfied (explicit miss).

2.4 Classification of findings

17. The examiners used the following classification for their findings:

- **Fail** - The finding identifies a failure to produce evidence of satisfying a requirement.
- **Partially fail** - The finding identifies a partial failure to produce evidence of satisfying a requirement.
- **Potential improvement** - The finding identifies a notable opportunity for improvement or optimisation.

18. Readers should note that the classification of findings indicated in this report only reflects the opinion of the examiners and may be subject to re-evaluation from relevant parties.

2.5 Relevance of the assessment criteria

19. The examiners raised an issue when the wording of a given requirement set in the OEV was perceived as unclear, or subject to interpretation, preventing the examiners from performing an objective assessment of the criterion.

2.6 Assumptions

2.6.1 Trustworthiness of statements

20. The examiners assume that the examinees were honest and transparent when providing answers to the examiners' assessment questions. No observation of the actual implementation of the OEV's requirements within the e-voting system was carried out to verify the accuracy of the examinees' statements.

2.6.2 Enforcement of security measures

21. The examiners assume that the security measures described in the documents provided as evidence in the context of the present examination are implemented and are effective. No observation of the actual implementation of the OEV's requirements within the e-voting system was carried out to verify the accuracy of the statements made in the security documents.

3 Impact analysis of release 1.5

22. The first step of the assessment consisted of identifying the impact areas of the e-voting software version 1.5 in relation to the OEV requirements applicable to the cantons. For this purpose, the examiners analysed the corresponding release note [14], categorised the identified changes and linked them to the relevant OEV requirements concerned. The outcome of this analysis is presented in the tables below.
23. While the changes introduced in release 1.5 may indirectly relate to additional OEV requirements, the analysis deliberately focused on those requirements for which a direct and sufficiently substantiated link to the documented changes could be established.

Key	A
Change in R1.5	Dispute detection and resolution in the tally process
Details	Implementation of a dispute resolver to detect and resolve inconsistent views of confirmed votes across control components, including new extraction algorithms (ExtractElectionEvent, ExtractVerificationCardSet, ExtractVerificationCards) and consistency-checking algorithms (CheckExtractedElectionEventConsistency, CheckVoteConsistency, CheckVoteConfirmationConsistency), as well as UpdateConfirmedVotingCards.
Impact	<p>Positive impact on integrity and universal verifiability: inconsistencies caused by configuration errors or internal manipulation are now detected and resolved at the start of the tally process.</p> <p>With regard to OEV requirements, the cantons must ensure, under Art. 11 OEV, that the published source code and system documentation reflect the newly introduced dispute resolution mechanisms.</p> <p>As the cantons apply the OCTAVE Allegro methodology for risk assessment, the dispute resolver can be considered an information asset within this framework. Consequently, the risk assessment mandated under §13 requires reassessment to take this new component into account.</p> <p>The cantons may also take into consideration the reduced exposure to risks related to internal manipulation and consistency errors resulting from the introduction of the dispute resolver.</p> <p>The dispute resolver is a software component installed on the replacement PC within the e-voting infrastructure. As such, it is subject to the same installation, configuration, integrity verification, hardening and operational constraints as other software components deployed in this environment, as defined in the applicable hardware and infrastructure requirements.</p> <p>Furthermore, cantonal personnel involved in the management of e-voting ballots must be familiar with the dispute resolution process, in line with the training and awareness requirements set out in §8.14 and §25.6.2.</p> <p>Finally, in cases where discrepancies between control components concerning confirmed votes are detected, an incident management procedure must be applied, in accordance with the relevant OEV requirements, notably §11.1 and §14.1.</p>

Impacted OEV chapters	Art.11, §2.6, 3.6, 3.7, 3.9, 3.10, 3.11, 3.14, 3.17, 3.20, 8.14, 11.1, 19.1, 14.1, 25.6.2
------------------------------	---

Table 1 – Impact analysis related to the introduction of a dispute resolver

Key	B
Change in R1.5	Other cryptographic and verifiability improvements
Details	<p>The following cryptographic and verifiability improvements have been introduced:</p> <ul style="list-style-type: none"> ■ Zero-knowledge proof verification for configuration data performed directly by the control components during system setup (using the <code>CombineEncLongCodeShares</code> algorithm), instead of being deferred to the external Verifier tool, ■ Use of <code>GetHashExtractedElectionEvent</code> in <code>PartialDecryptPCC</code> and <code>DecryptPCC</code> to bind partial decryption operations to the hash of the extracted election event, ■ Use of the new algorithms <code>GenXMLSignature</code> and <code>VerifyXMLSignature</code> for all XML interfaces.
Impact	<p>Positive impact on integrity and verifiability of the system: cryptographic checks are strengthened by binding critical operations (configuration validation, partial decryption, and XML interface handling) more tightly to trusted election data and to formally verified algorithms executed by the control components. The verification of zero-knowledge proofs during the configuration phase is now performed directly by the control components, rather than being deferred to the external Verifier tool, reducing the risk that malformed or inconsistent cryptographic data propagate unnoticed into later phases.</p> <p>The use of <code>GetHashExtractedElectionEvent</code> in <code>PartialDecryptPCC</code> and <code>DecryptPCC</code> further strengthens context binding between decryption operations and the extracted election event, reducing the risk of mismatches or manipulation of contextual data during the tally.</p> <p>The introduction of the <code>GenXMLSignature</code> and <code>VerifyXMLSignature</code> algorithms standardises the generation and verification of XML signatures across configuration, printing and result interfaces, improving the consistency and robustness of integrity checks.</p> <p>There is no change to operational procedures for the cantons. Cantonal staff and auditors continue to rely on the Verifier as a technical aid to verify evidence and results. Under Art. 11 OEV, the cantons must ensure that the published source code and system documentation, are updated to consider these cryptographic improvements and that the algorithms used correspond to the state of the art. The cantons may also take into account the reduced exposure to cryptographic integrity and context-binding errors in their risk assessment</p>
Impacted OEV chapters	Art.11, §2.6, 13.8, 13.9, 13.10, 13.31, 13.32, 15.2, 15.4

Table 2 – Impact analysis related to other cryptographic and verifiability improvements

Key	C
Change in R1.5	Voting client codebase hardening and dependency reduction

Details	Migration of the voting client to TypeScript, removal of remaining JavaScript modules and lodash dependency, and renaming of the package from voting-client-js to voting-client.
Impact	<p>No operational impact for the cantons: cantonal procedures and responsibilities remain unchanged. In particular, the Trusted Build process is applied in the same way, with no modification to the steps used to rebuild the voting client from the published source code and verify its integrity.</p> <p>Under Art. 11 OEV, the cantons must ensure that the published source code and software documentation (incl. trusted-build instructions) reflect the updated client implementation.</p> <p>The cantons should also consider the reduced dependency-related risks in their risk assessment.</p>
Impacted OEV chapters	Art.11, §13.3, 13.6, 13.19.

Table 3 – Impact analysis related to voting client codebase hardening and dependency reduction

Key	D
Change in R1.5	Voter portal usability and robustness improvements
Details	<p>These changes implement measure A.19 of the Federal Chancellery’s improvement catalogue by reducing cognitive load for voters and making the verification steps more visible and comprehensible:</p> <ul style="list-style-type: none"> ■ Alignment of the portal layout and terminology with the printed voting card, ■ Separation of the verification of return codes from the entry of the ballot casting key, ■ Introduction of a dedicated finalisation page, ■ Improvement of UX elements for popular votes and elections, ■ Improved validation of election events when accessing the voter portal, ■ Improved checks for device compatibility, ■ More robust handling of repeated vote confirmation requests.
Impact	<p>Positive impact on usability and individual verifiability: voters are more likely to correctly use the verification features and to notice anomalies if their vote has been manipulated or miscast.</p> <p>There is no change to the canton’s operational procedures, but voter information materials and training may need to be adapted to reflect the updated portal flow and terminology.</p> <p>The cantons may also consider the reduced usability- and verification-related risks in their risk assessment.</p>
Impacted OEV chapters	§8.3, 13.12, 13.16, 13.35, 13.37, 13.38, 13.40.

Table 4 – Impact analysis related to voter portal usability and robustness improvements

Key	E
Change in R1.5	Result handling, formats and result presentation
Details	<ul style="list-style-type: none"> ■ Removal of the generation of evoting-decryption files.

Impact	<ul style="list-style-type: none"> ■ Removal of the generation of eCH-0110 XML result files. ■ Adding of a detailed per ballot box display of the election event result (for popular votes and elections).
	<p>Result data are now provided exclusively in the eCH-0222 format, which is specifically designed for e-voting and can carry both the result data and the associated technical metadata (e.g. context information, hashes, verifiability-related data). In contrast, eCH-0110 is a generic result format that does not model the e-voting protocol structures as precisely. The changes clarify and standardise how XML signatures are computed and verified for these files. The cantons may also consider the reduced integrity- and authenticity-related risks for these XML interfaces in their risk assessment.</p> <p>The removal of the eCH-0110 and e-voting-decryptio files changes the result-verification steps performed by Admin- and Electoral-Board members during D3. The new way of displaying results has a limited impact on the interpretation of results. The canton must adapt the training programme and training environment so that staff and auditors are trained on the updated process and on the exclusive use of the eCH-0222 result file, in line with OEV requirements 8.14 and 25.6.2–25.6.4. Under Art. 11 OEV, the cantons must ensure that the published source code and software documentation reflect these changes.</p>
Impacted OEV chapters	Art.11, §3.3, 8.14, 25.6.2–25.6.4

Table 5 – Impact analysis related to result handling, formats and result presentation

Key	F
Change in R1.5	Platform, infrastructure and scalability changes
Details	<ul style="list-style-type: none"> ■ Introduction of multi-tenancy support, ■ Database management refactoring + migration from Oracle to PostgreSQL, ■ Streamlined import of an election event into the Secure Data manager + migration of the DB from Orient DB to SQLite, ■ Improved robustness when handling very large election events, ■ Dependencies and third-party libraries updates, ■ Small improvements and bug fixes.
Impact	<p>No operational impact for the cantons: the platform, infrastructure and scalability changes do not introduce any new canton-facing operational steps.</p> <p>The cantons must ensure, under Art. 11 OEV, that the published source code and system documentation provided by Swiss Post reflect the updated platform architecture and infrastructure components. The cantons should also take into account the reduced risks related to scalability limits, platform robustness, dependency management and bug fixes in their risk assessment.</p>
Impacted OEV chapters	Art.11, §13.7, 13.10, 13.18, 13.19, 13.31, 13.33.

Table 6 – Impact analysis related to platform, infrastructure and scalability changes

4 Assessment results

24. The following tables present the results of the compliance assessment performed against the requirements identified in the previous chapter.
25. For the sake of clarity, the observations related to to each selected OEV requirement focus exclusively on the impact of the changes introduced in version 1.5 of the software and do not reassess the overall compliance status of that requirement beyond the scope of these changes.

Art 11

Key	Art.11
Requirement	<p>Art. 11 Disclosure of the source code and of the documentation on the system and its operation</p> <p>1 The canton shall ensure that the following documents are published:</p> <ul style="list-style-type: none"> a. the source code of the system software including files with relevant parameters; b. evidence that the machine-readable programmes were generated from the published software source code; c. the software documentation; d the development process documentation; e. instructions and other documents that experts require to be able to compile, execute and analyse the system on the basis of the source code within their own infrastructure; f. technical specifications of the main components of the system; g. the process documentation for operating, maintaining and securing the system; h. information on and descriptions of known flaws. <p>2 The following need not be published:</p> <ul style="list-style-type: none"> a. the source code for third-party components such as operating systems, databases, web and application servers, rights management systems, firewalls or routers, provided they are widely used and regularly updated; b. the source code for portals of authorities that are connected to the system; c. documents or parts of documents for which an exemption from publication is justified, in particular under the law on freedom of information or data protection.
Observation (R1.5 changes)	In step 0.1 of the <i>Prozesse E-Voting</i> document, the cantons verify that the source code and the documentation on the system and its operation are published by Swiss Post. This check occurs 160 to 80 days before the ballot takes place.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.11, step 0.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 7 – Examination results: OEV Art.11

Requirement for the cryptographic protocol: universal verifiability

Key	2.6
Requirement	The auditors receive a proof in accordance with Article 5 paragraph 3 letter a in conjunction with Article 6 letters a and c to confirm that no attacker: <ul style="list-style-type: none"> ■ after the votes were registered as cast in conformity with the system, has altered or misappropriated any partial votes before the result was determined; ■ has inserted any votes or partial votes not cast in conformity with the system which were taken into account in determining the result.
Observation (R1.5 changes)	The dispute resolver and the cryptographic improvements introduced in release 1.5 reinforce universal verifiability by strengthening the consistency checks and the cryptographic binding of election data, thereby improving the robustness of the proofs provided to auditors.
Evidence	N/A
Result	Pass
Finding	N/A
Relevance	N/A

Table 8 – Examination results: OEV paragraph 2.6

Requirements for trustworthy components in accordance with Number 2 and for their operation

Key	3.3
Requirement	Auditors must verify the proofs referred to in Number 2.6 at least once and must use a technical aid referred to in Number 2 for this purpose.
Observation (R1.5 changes)	The <i>E-Voting - Konzept Vollständige Verifizierbarkeit</i> document has been updated and now refers to the eCH-0222 format regarding the verification of the proofs.
Evidence	BS, GR, SG, TG: E-Voting - Konzept Vollständige Verifizierbarkeit - V1.8, §3.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 9 – Examination results: OEV paragraph 3.3

Keys	3.6, 3.7, 3.9, 3.10, 3.11, 3.14, 3.17, 3.20
Requirements	3.6: Trustworthy components (set-up components, print components, auditors' technical aids and control components) must be set up, updated, configured and secured in an observable process. 3.7: Before installing software, all programs must be checked using an official and trustworthy reference to ensure that the files are the correct and unaltered version.

	<p>3.9: The timing for updating all software of trustworthy components must be such that the expected benefits outweigh the potential hazards.</p> <p>3.10: Set-up components, print components and auditors' technical aids that are involved in any way in the processing of critical data must be physically monitored during the entire computing time by two persons and until any critical data have been deleted or securely stored. At most, they may be interconnected by visible physical cables so that it is as evident as possible that no other machines can access them until the confidential data is destroyed.</p> <p>3.11: Trustworthy components may not be connected to the internet when installing or updating software.</p> <p>3.14: Logical or physical access to trustworthy components or data carriers containing critical data must be impossible without another person becoming aware of it, for example by having to assist in granting access (strict two-person principle).</p> <p>3.17: Trustworthy components may perform only the intended operations.</p> <p>3.20: Any access to and use of a trusted component or data carrier containing critical data must be logged.</p>
Observation (R1.5 changes)	The dispute resolver software component is installed on the existing environment dedicated to e-voting operations (i.e., on the replacement PC), in accordance with the installation and operational principles already in place. The introduction of this new piece of software does therefore not affect the compliance level of the cantons with the requirements related to the operation of trustworthy components.
Evidence	<ul style="list-style-type: none"> ■ BS: E-Voting BS - Hardware und Infrastruktur – V1.9, §4, 6 ■ GR: E-Voting - Hardware und Infrastruktur – V1.5, §5, 7 ■ SG: E-Voting - Hardware und Infrastruktur – V1.8, §5, 7 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.8, §5, 7 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.11, step 0.3.2, 0.3.4, §4.4
Result	Pass
Finding	N/A
Relevance	N/A

Table 10 – Examination results: OEV paragraph 3.6, 3.7, 3.9, 3.10, 3.11, 3.14, 3.17, 3.20

Information and instructions

Key	8.3
Requirement	Tips and instructions on vote casting are given on the internet along with information on voters' responsibilities. This should counter over-hasty or ill-considered vote casting behaviour.
Observation (R1.5 changes)	The usability improvements introduced in release 1.5 support this requirement by improving the clarity and visibility of voting and verification instructions provided to voters, thereby reducing the risk of hasty or ill-informed vote casting.
Evidence	N/A
Result	Pass
Finding	N/A
Relevance	N/A

Table 11 – Examination results: OEV paragraph 8.3

Key	8.14
Requirement	The auditors should be suitably informed about and trained in the processes that determine the accuracy of the result, the preservation of voting secrecy and the exclusion of premature partial results (for example key generation, printing the voting papers, decryption and tallying). They must be able to understand the essential aspects of the processes and their significance.
Observation (R1.5 changes)	<p>The training concept explicitly provides for the update of training content in the event of significant technological or procedural changes, and for the re-delivery of training sessions where such changes affect the roles, processes or verification activities performed by the participants.</p> <p>In particular, the training framework for members of the Electoral Board covers the processes related to universal verifiability, the use of the Verifier, the plausibilisation of results, and the handling of anomalies and incidents. This framework allows newly introduced mechanisms, such as the dispute resolution process and the related changes to tallying and verification workflows, to be incorporated into the training materials and refresher sessions.</p> <p>Similarly, the training and “training-on-the-job” activities defined for the Admin Board, including test runs and voting tests, provide a mechanism to familiarise the involved personnel with procedural and technical changes introduced by the new release.</p>
Evidence	<ul style="list-style-type: none"> ■ BS: E-Voting BS - Konzept Schulungen und interne Information – V1.1, §1.13 ■ GR: E-Voting - Konzept Schulungen und interne Information – V1.1, §2.13 ■ SG: E-Voting - Konzept Schulungen und interne Information – V1.1, §2.13 ■ TG: E-Voting-TG-Konzept-Schulungen-und-interne-Information – V1.1, §2.13
Result	Pass
Finding	N/A
Relevance	N/A

Table 12 – Examination results: OEV paragraph 8.14

Tallying votes in the electronic ballot box

Key	11.11
Requirement	The canton anticipates any anomalies and, in consultation with the bodies concerned, draws up an emergency plan specifying the appropriate course of action. It creates transparency towards the public.
Observation (R1.5 changes)	<p>The cantons, in collaboration with the Post (the e-voting system provider), maintain an emergency plan detailing the steps to perform in case of potential anomalies. The emergency plan of the cantons mentions the publication of its anomaly analyses.</p> <p>In this context, the user guide provided by Swiss Post further documents a predefined procedure applicable to a specific anomaly scenario involving discrepancies between control components (dispute resolver), thereby providing additional operational guidance relevant to the implementation of such emergency plans.</p>
Evidence	BS, GR, SG, TG: Benutzeranleitung Release 1.5, §9.7
Result	Pass

Finding	N/A
Relevance	N/A

Table 13 – Examination results: OEV paragraph 11.11

Threats

Key	13.1
Requirement	The threats listed in Numbers 13.3-13.40 are of a general nature and form a minimum basis; this must be added to. They relate to the security objectives and must be taken into account when identifying risks. Depending on the system vulnerabilities identified, when the various bodies carry out their risk assessments, the list should be updated with full details and considered based on the actual circumstances and depending on the specific threat.
Observation (R1.5 changes)	The cantons have reviewed their risk portfolio following the introduction of version 1.5 of the e-voting software. However, the improvements introduced by this release have not been reflected in the corresponding risk evaluations.
Evidence	<ul style="list-style-type: none"> ■ BS, GR, SG, TG: E-Voting - Änderungsliste Risikobeurteilung ■ BS, GR, SG, TG: Risk portfolio (04.12.2025)
Result	Potential improvement
Finding	The improvements introduced by the 1.5 release of the e-voting software have not been reflected in the corresponding risk evaluations.
Relevance	The requirement includes a translation error: “this must be added to” (German version: “,die zu ergänzen ist”)

Table 14 – Examination results: OEV paragraph 13.1

Identifying and reporting security events and vulnerabilities; dealing with security events and making security improvements

Key	14.1
Requirement	<p>An infrastructure monitoring system detects incidents that could endanger the security, including availability, of the system and alerts the responsible personnel. The personnel deal with incidents according to a predetermined procedure. Crisis scenarios and rescue plans serve as guidelines (and include a plan that guarantees that voting-related activities can continue) and are applied as required.</p> <p>Errors in the registration of votes in the control components and in the ballot box must be detected. Further information relating to the error must be available in order to identify and eliminate the cause. Any incidents detected must be reported to the body responsible at cantonal level.</p>
Observation (R1.5 changes)	The user guide provided by Swiss Post documents a predefined procedure to be followed when discrepancies between control components regarding confirmed votes are detected (Dispute Resolver procedure). The documented steps cover reporting, analysis, execution on the reserve workstation, secure data exchange, and the resumption of tallying once the discrepancy has been resolved.
Evidence	BS, GR, SG, TG: Benutzeranleitung Release 1.5 §9.7
Result	Pass

Finding	N/A
Relevance	N/A

Table 15 – Examination results: OEV paragraph 14.1

Key	14.9
Requirement	All parts of the voting system must be regularly updated in a predetermined and documented process in order to eliminate weaknesses that have become known.
Observation (R1.5 changes)	The dispute resolver software component is installed on the replacement PC within the existing e-voting infrastructure and is subject to the same update and maintenance procedures as the other software components deployed on this environment.
Evidence	<ul style="list-style-type: none"> ■ BS: E-Voting BS - Hardware und Infrastruktur – V1.9, §4 ■ GR: E-Voting - Hardware und Infrastruktur – V1.5, §5 ■ SG: E-Voting - Hardware und Infrastruktur – V1.8, §5 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.8, §5 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.11, step 0.3.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 16 – Examination results: OEV paragraph 14.9

Use of cryptographic measures and key management

Key	15.2
Requirement	In order to guarantee the integrity of data records that substantiate the accuracy of the result and ensure that critical data, including the authorities' identification and authentication data, are kept secret, effective cryptographic measures that correspond to the state of the art must be used.
Observation (R1.5 changes)	The cryptographic improvements introduced in release 1.5 strengthen the integrity and robustness of election data and related cryptographic operations by relying on state-of-the-art mechanisms, as detailed in the documentation provided by Swiss Post.
Evidence	BS, GR, SG, TG: Swiss Post Voting System – System Specification - v1.5.2, §3.6, 4.1.6, 5.2.3, 5.2.4, 7.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 17 – Examination results: OEV paragraph 15.2

Key	15.4
------------	------

Requirement	Basic cryptographic components may only be used if the key lengths and algorithms correspond to the current standards (e.g. NIST, ECRYPT, ESigA). The electronic signature meets the requirements of an advanced electronic signature in accordance with the Federal Act of 18 March 2016 on Electronic Signatures (ESigA). The signature must be verified by means of an electronic certificate that has been issued by a recognised supplier of certificate services under the ESigA.
Observation (R1.5 changes)	The algorithms and key lengths used by the cryptographic components introduced in release 1.5 correspond to current standards, as detailed in the documentation provided by Swiss Post.
Evidence	BS, GR, SG, TG: Cryptographic Primitives of the Swiss Post Voting System – 1.5.1, Table 3: Primitives and their parametrization
Result	Pass
Finding	N/A
Relevance	N/A

Table 18 – Examination results: OEV paragraph 15.4

Secure electronic and physical exchange of information

Key	16.2
Requirement	As a principle, electronic voting should be clearly separated from all other applications.
Observation (R1.5 changes)	The dispute resolver runs on the replacement PC, which is dedicated to e-voting operations.
Evidence	<ul style="list-style-type: none"> ■ BS: E-Voting BS - Hardware und Infrastruktur – V1.9, §3 ■ GR: E-Voting - Hardware und Infrastruktur – V1.5, §4 ■ SG: E-Voting - Hardware und Infrastruktur – V1.8, §4 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.8, §4
Result	Pass
Finding	N/A
Relevance	N/A

Table 19 – Examination results: OEV paragraph 16.2

Organisation of information security

Key	18.1
Requirement	All roles and responsibilities for the operation of the system must be precisely defined, assigned and communicated.
Observation (R1.5 changes)	The <i>Prozesse E-Voting</i> document refers to the possible use of a dispute resolver in the event of a conflict between control components during the vote mixing phase. This operation is carried out by the Admin-Board.
Evidence	BS, GR, SG, TG: Prozesse E-Voting V1.11, step 3.3.1
Result	Pass

Finding	N/A
Relevance	N/A

Table 20 – Examination results: OEV paragraph 18.1

Key	18.2
Requirement	The initial configuration of the infrastructure, whether with regard to hardware, software or access rights, and any modification must be approved beforehand.
Observation (R1.5 changes)	As the dispute resolver software is installed on the existing infrastructure (replacement PC), the installation process is subject to the existing authorisation process.
Evidence	<ul style="list-style-type: none"> ■ BS, GR, SG, TG: Prozesse E-Voting V1.11, step 0.3.2 ■ BS: E-Voting BS - Hardware und Infrastruktur – V1.9, §4 ■ GR: E-Voting - Hardware und Infrastruktur – V1.5, §5 ■ SG: E-Voting - Hardware und Infrastruktur – V1.8, §5 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.8, §5
Result	Pass
Finding	N/A
Relevance	N/A

Table 21 – Examination results: OEV paragraph 18.2

Management of intangible and tangible resources

Key	19.1
Requirement	All intangible and tangible resources in the sense of the term asset in the standard ISO/IEC 27001, 2013, Information technology - Security techniques - Information security management systems - Requirements , relevant in the context of electronic voting (organisation as a whole, in particular the organisational processes and the information processed in these processes, data carriers, facilities for processing information of the infrastructure and premises of the infrastructure) are recorded in an inventory. A list must be kept of human resources. The inventory and human resources list must be kept up to date. Each intangible and tangible resource is assigned a person who takes responsibility for it.
Observation (R1.5 changes)	The cantons have added a new entry: <i>data for dispute resolver</i> to their existing inventory of information assets, which serves as an input to their risk assessment.
Evidence	BS, GR, SG, TG: E-Voting - Inventar der Informationsressourcen (04.12.2025)
Result	Pass
Finding	N/A
Relevance	N/A

Table 22 – Examination results: OEV paragraph 19.1

Key	21.3
------------	------

Requirement	To guarantee the security of devices within and outside the infrastructure premises, appropriate policies and procedures must be defined and compliance therewith monitored and reviewed.
Observation (R1.5 changes)	The <i>Hardware und Infrastruktur</i> document includes chapters regarding the physical security measures aimed at protecting the e-voting infrastructure (e.g. perimeter security, access rules, surveillance principles, secure storage, logging of actions performed, etc.). The <i>Richtlinie Informationssicherheit</i> document mentions that the electoral board monitors and has a right to audit the compliance with established rules regarding physical security.
Evidence	<ul style="list-style-type: none"> ■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.4 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.4 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.4 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4.4 ■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §5, 6 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §6, 7 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §6, 7 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §6, 7
Result	Pass
Finding	N/A
Relevance	N/A

Table 23 – Examination results: OEV paragraph 21.3

Learnability

Key	25.6.2 – 25-6.4
Requirements	<p>25.6.2: Persons who operate and use the system must be trained and provided with the necessary documentation.</p> <p>25.6.3: Training includes the opportunity to train on a system designed for training purposes.</p> <p>25.6.4: Help on using the system must be readily available.</p>
Observation (R1.5 changes)	<p>The training concept defines a structured framework to ensure that persons operating and using the e-voting system are trained and provided with the necessary documentation. It covers both the Electoral Board and the Admin Board and explicitly foresees the update and re-delivery of training content and materials in the event of significant technological or procedural changes.</p> <p>The changes introduced with release 1.5 affect the handling and verification of election results, in particular through the exclusive use of the eCH-0222 result file and the removal of the eCH-0110 and e-voting-decryption files, which modify certain verification steps performed during D3 without introducing new roles or fundamentally new verification objectives.</p> <p>The training framework includes opportunities to practise on a dedicated test environment through test runs and voting tests, allowing the updated result handling and verification procedures to be exercised prior to productive use. In addition, supporting documentation, checklists and relevant technical documentation are made available to the involved personnel to assist them in performing their tasks.</p>

Evidence	<ul style="list-style-type: none"> ■ BS: E-Voting BS - Konzept Schulungen und interne Information – V1.1 ■ GR: E-Voting - Konzept Schulungen und interne Information – V1.1 ■ SG: E-Voting - Konzept Schulungen und interne Information – V1.1 ■ TG: E-Voting-TG-Konzept-Schulungen-und-interne-Information – V1.1 ■ BS, GR, SG, TG: Benutzeranleitung Release 1.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 24 – Examination results: OEV paragraph 25.6.2-25.6.4

5 Summary of findings and recommendations

26. This section recaps the findings made during the examination, their severity, and provides succinct recommendations to address them.

Key	13.1
Requirement	The threats listed in Numbers 13.3-13.40 are of a general nature and form a minimum basis; this must be added to. They relate to the security objectives and must be taken into account when identifying risks. Depending on the system vulnerabilities identified, when the various bodies carry out their risk assessments, the list should be updated with full details and considered based on the actual circumstances and depending on the specific threat.
Finding	The improvements introduced by the 1.5 release of the e-voting software have not been reflected in the corresponding risk evaluations.
Recommendation	The cantons should update the <i>Erläuterungen</i> section of the relevant risks in their portfolio to reflect the reduced likelihood of occurrence resulting from the improvements introduced in release 1.5 of the e-voting software, even where the likelihood rating itself remains unchanged.

Table 25 – Finding related to requirement 13.1

6 References

- [1] “Swiss Citizens should be able to vote electronically,” Administration numérique suisse, [Online]. Available: <https://www.digital-public-services-switzerland.ch/en/implementation/egovernment-implementation-plan/redesigning-evoting>. [Accessed 22 May 2024].
- [2] “Redesign and relaunch of trials - Final report of the Steering Committee Vote électronique (SC VE),” Swiss Federal Chancellery, Political Rights Section, 30 November 2020. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/Final%20report%20SC%20VE_November%202020.pdf.download.pdf/Final%20report%20SC%20VE_November%202020.pdf. [Accessed 22 May 2024].
- [3] “Partial revision of the Ordinance on Political Rights and total revision of the Federal Chancellery Ordinance on Electronic Voting (Redesign of Trials),” Swiss Federal Chancellery, Political Rights Section, 28 April 2021. [Online]. Available: <https://www.bk.admin.ch/dam/bk/en/dokumente/pore/Explanatory%20report%20for%20consultation%202021.pdf.download.pdf/Explanatory%20report%20for%20consultation%202021.pdf>. [Accessed 22 May 2024].
- [4] “Federal Chancellery ordinance on electronic voting (OEV),” Swiss Federal Chancellery, 21 April 2021. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/OEV_draft%20for%20consultation%202021.pdf.download.pdf/OEV_draft%20for%20consultation%202021.pdf. [Accessed 22 May 2024].
- [5] “Audit concept v1.3 for examining Swiss Internet voting systems,” Federal Chancellery (FCh), Political Rights Section, 18 May 2021. [Online]. Available: <https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Audit%20concept,%2018.05.2021.pdf.download.pdf/Audit%20concept,%2018.05.2021.pdf>. [Accessed 22 May 2024].
- [6] “Ordinance on Political Rights (PoRo). section 6a: Electronic Voting Trials,” Swiss Federal Chancellery, [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/PoRO_Section%206a%20on%20Electronic%20Voting%20Trials.pdf.download.pdf/PoRO_Section%206a%20on%20Electronic%20Voting%20Trials.pdf. [Accessed 22 May 2024].
- [7] “Federal Chancellery Ordinance on Electronic Voting (OEV),” Swiss Federal Chancellery, 25 May 2022. [Online]. Available: <https://www.fedlex.admin.ch/eli/cc/2022/336/en>. [Accessed 22 May 2024].
- [8] “Audit concept v1.5 for examining Swiss internet voting systems,” Federal Chancellery (FCh), Political Rights Section, 15 September 2022. [Online]. Available:

<https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Vote--lectronique/Audit%20concept%20v1.5.pdf.download.pdf/Audit%20concept%20v1.5.pdf>. [Accessed 22 May 2024].

- [9] “Federal Council authorises use of online voting in 2023 National Council elections,” The federal Council, 18 August 2023. [Online]. Available: <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-97361.html>. [Accessed 22 May 2024].
- [10] “Federal Council authorises use of online voting in the canton of Graubünden,” The Federal Council, 22 November 2023. [Online]. Available: <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-98768.html>. [Accessed 22 May 2024].
- [11] “Examination of the Swiss Internet voting system v1.0 /Audit scope: Infrastructure and operations (3) - Measures of the canton,” SCRT, 17 February 2023. [Online]. Available: [https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_Reports_March2023/Scope%203%20\(Cantons\)%20Final%20Report%20SCRT%2017.02.2023.pdf.download.pdf/Scope%203%20\(Cantons\)%20Final%20Report%20SCRT%2017.02.2023.pdf](https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_Reports_March2023/Scope%203%20(Cantons)%20Final%20Report%20SCRT%2017.02.2023.pdf.download.pdf/Scope%203%20(Cantons)%20Final%20Report%20SCRT%2017.02.2023.pdf). [Accessed 22 May 2024].
- [12] “Examination of the Swiss internet voting system / Audit scope: Infrastructure and operations (3) - Measures of the canton,” SCRT, 3 November 2023. [Online]. Available: [https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_reports_November2023/Scope%203%20\(Canton%20GR\)%20Final%20Report%20SCRT%2003.11.2023.pdf.download.pdf/Scope%203%20\(Canton%20GR\)%20Final%20Report%20SCRT%2003.11.2023.pdf](https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_reports_November2023/Scope%203%20(Canton%20GR)%20Final%20Report%20SCRT%2003.11.2023.pdf.download.pdf/Scope%203%20(Canton%20GR)%20Final%20Report%20SCRT%2003.11.2023.pdf). [Accessed 22 May 2024].
- [13] “Audit concept v1.6 for examining Swiss Internet voting systems,” Federal Chancellery (FCh), Political Rights Section, 7 February 2025. [Online].
- [14] S. Post, “CHANGELOGmd,” Swiss Post, 2025. [Online]. Available: <https://gitlab.com/swisspost-evoting/e-voting/e-voting/-/blob/master/CHANGELOG.md>. [Accessed 17 December 2025].