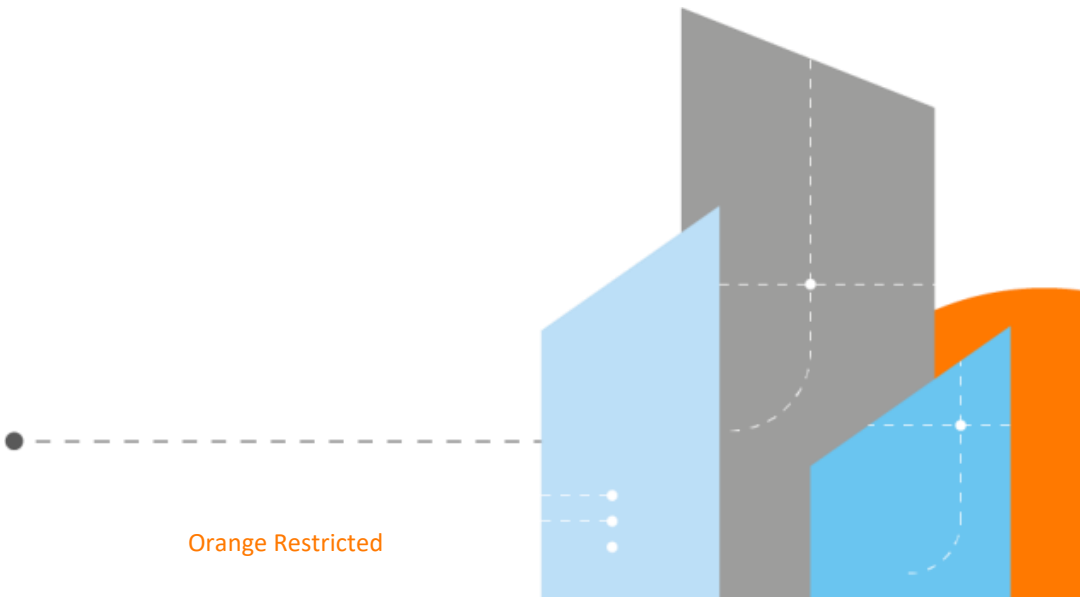
Cyberdefense

Federal Chancellery

Examination of the Swiss Internet voting system

Version: 1.1 / Audit scope: Infrastructure and operations (3) – Measures of the canton

23 May 2025



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@orangecyberdefense.com

Contributors

Name	Role
Stéphane Adamiste	Chief Product Officer, Orange Cyberdefense Switzerland

Document history

Version	Date	Author	Change details
0.1	21 February 2025	Stéphane Adamiste	Working version
1.0	17 April 2025	Stéphane Adamiste	Released version
1.1	23 May 2025	Stéphane Adamiste	Integration of the cantons' feedback

Contents

Management summary

Context, scope and objective of the examination

Following a first audit in 2022 and partial audits in 2023 and 2024, the objective of this examination was to fully re-assess the extent to which infrastructure and organisational measures supporting the operation of the Swiss Post's e-voting system in the cantons of Basel Stadt, Graubünden, St. Gallen and Thurgau satisfy a subset of requirements (*audit scope 3 - Infrastructure and operation, c) Assess the infrastructure and organisational measures of the cantons*) set forth by the Federal Chancellery's ordinance on e-voting. In total, the examination work included 171 criteria.

Methodology

The examiners looked for evidence of effort to comply with said criteria through interviews of the personnel in charge of the setup and operation of the e-voting system's infrastructure at cantonal level, by analysing the related documentation (i.e., policies, procedures, specifications, reports, processes, etc.) and by observing the entire process of a test ballot.

Results

Overall, the cantons have demonstrated a high level of compliance with the applicable requirements of the ordinance on e-voting: One non-compliance, one partial non-compliance and one potential improvement were identified. It is worth noting that the cantons rely on the Swiss Post for the resolution of the non-compliance and that the partial non-compliance does not present a security risk.

Recommendations

Only succinct recommendations are provided in this document, as the observations formulated are self-explanatory. In the examiners' opinion, implementing those recommendations requires only limited effort considering the scale of the e-voting project.

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]

2 Methodology

2.1 Process

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

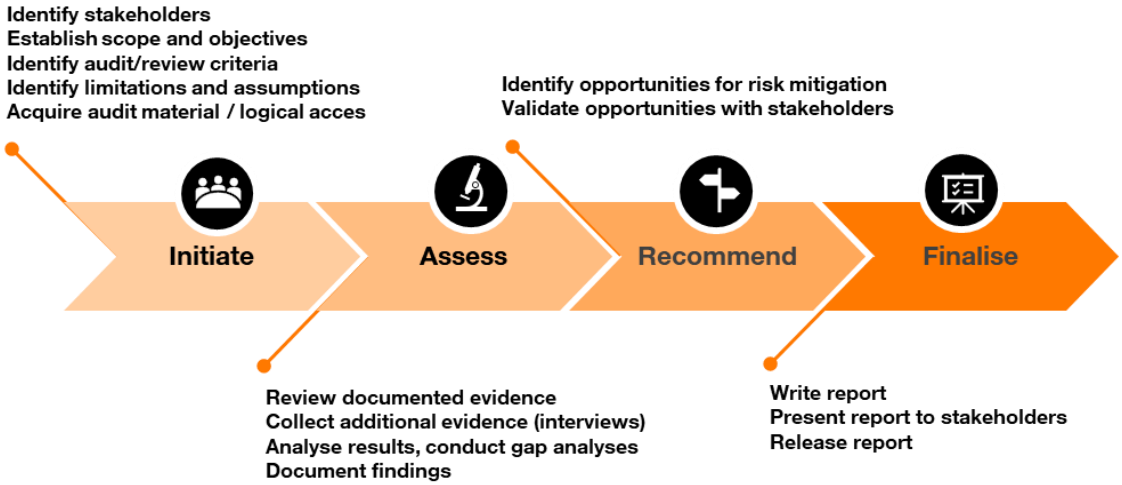


Figure 1: Examination process

2.2 Collection of evidence

14. 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

15. 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

16. 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.

17. 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

18. 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

19. The examiners assume that the examinees were honest and transparent when providing answers to the examiners' assessment questions. The observation of the actual implementation of the OEV's requirements within the e-voting system was limited to the demo made by the e-voting representatives of the Thurgau canton carried out to verify the accuracy of the examinees' statements.

2.6.2 Enforcement of security measures

20. 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 Examination criteria

21. This examination focussed on assessing the compliance of the Swiss Post's e-voting system from the cantons' standpoint against the following criteria:

Art. 11[1]

Key	Requirement
Art. 11	**Disclosure of the source code and of the documentation on the system and its operation** 1 The canton shall ensure that the following documents are published: 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. 2 The following need not be published: 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.

Table 1 - E-voting requirements: Art. 11

Art 14

Key	Requirement
Art. 14	**Responsibility for running the ballot with electronic voting correctly** 1 The canton bears overall responsibility for running the ballot with electronic voting correctly. 2 It must carry out important tasks itself. 3 It may delegate the development of the software used, technical operational tasks and communication on questions about how the system works to external organisations.

Table 2 - E-voting requirements: Art. 14

[1] Although this article is not listed in the audit concept as a requirement applicable to the canton, compliance with it has been evaluated by the examiners upon explicit request by the Federal Chancellery.

Cryptographic protocol requirements for complete verifiability

Key	Requirement
2.5	**Requirement for the cryptographic protocol: individual verifiability** The voter is given proofs in accordance with Article 5 paragraph 2 in conjunction with Article 6 letters a and b to confirm that no attacker ■ has altered any partial vote before the vote has been registered as cast in conformity with the system; ■ has not maliciously cast a vote on the voter's behalf which has subsequently been registered as a vote cast in conformity with the system and counted.
2.6	**Requirement for the cryptographic protocol: universal verifiability** 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: ■ 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.
2.7.1	It must be ensured that no attacker is able to breach voting secrecy or establish premature partial results unless he can control the voters or their user devices.
2.7.2	There is no obligation to prevent attacks that limit the number of tallied votes to the degree that all partial votes for a question, list or candidate are the same.
2.7.3	It must be ensured that no attacker can take control of user devices unnoticed by manipulating the user device software on the server. The person voting must be able to verify that the server has provided his or her user device with the correct software with the correct parameters, in particular the public key for encrypting the vote.
2.8	**Requirement for the cryptographic protocol: effective authentication.** It must be ensured that no attacker can cast a vote in conformity with the system without having control over the voters concerned.
2.9.1.2	**For soundness of the proofs referred to in Number 2.5** The following system participants may be considered trustworthy: ■ set-up component ■ print component ■ one of four control components per group, leaving open which one it is
2.9.2.2	**For soundness of the proofs referred to in Number 2.6** The following system participants may be considered trustworthy: ■ one of four control components per group, leaving open which one it is ■ one auditor in any group, leaving open which auditor it is ■ one technical aid from a trustworthy auditor, leaving open which aid it is
2.9.3.2	**For preserving voting secrecy and excluding premature partial results in accordance with Number 2.7** It may be assumed that trustworthy channels exist to distribute electronic certificates among system participants. Number 3.8 applies.
2.13.3	**Requirements for the definition and description of the cryptographic protocol** It may be assumed that trustworthy channels exist to distribute electronic certificates among system participants. Number 3.8 applies.

Table 3 - E-voting requirements: Cryptographic protocol requirements for complete verifiability

Trustworthy components in accordance with Number 2 and for their operation

Key	Requirement
3.1	The operation of the set-up component and at least one control component in the group which contains part of the key for decrypting the votes is the direct responsibility of the canton and must take place within its infrastructure. Outsourcing to a private system operator is not permitted.
3.2	Sufficient entropy must be ensured when selecting random values, in particular for set-up components and control components.
3.3	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.
3.4	The operational requirements for set-up components in accordance with Number 3 also apply to technical aids used by the auditors. Within the scope of their responsibility under cantonal law, the auditors may provide for derogations.
3.5	With the exception of the components mentioned under Numbers 3.1 and 3.3, the canton may delegate the operation of any part of the system, including the control components and the print component, to private service providers. A private operator of the print component may only perform operational tasks that are required for preparation, packaging and delivery.
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.
3.8	When other system participants' electronic certificates are installed, their authenticity must be ensured. To that end, there should be a manual process in which people transfer the electronic certificates from one machine to another via a physical data carrier in accordance with 3.13.
3.9	The timing for updating all software of trustworthy components must be such that the expected benefits outweigh the potential hazards.
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.
3.11	Trustworthy components may not be connected to the internet when installing or updating software.
3.12	In principle, critical data must be destroyed after use. If there are good reasons, secure storage of the data carrier is also permitted as an alternative.
3.13	Data exchange or storage media, such as USB flash drives, must be removed after the data has been uploaded to the trustworthy components and may only be reused before the data is destroyed if there was no critical data on the trustworthy component before the data was uploaded. Data exchange or storage media must be reformatted and any data on them must be destroyed before they are used with the aid of a component operated in accordance with the requirements for trustworthy components.

Key	Requirement
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).
3.15	Success in gaining unauthorised access to a control component should not as far as possible give any advantage in an attempt to access another control component unnoticed. In addition to the requirements set out in Number 3, the following requirements apply in this respect: ■ If a person has physical or logical access to a control component, that person may not have access to any other control component. ■ The hardware, the operating systems and the monitoring systems for the control components should be as distinct as possible from each other. ■ The control components should be connected to different local networks. A control component must take the form of a physical device. Virtualisation across multiple physical devices is not permitted.
3.16	Control components must be designed to recognise unpermitted instances of access and to alert the persons responsible. The persons responsible should arrange external monitoring measures, such as the monitoring and the manipulation-resistant logging of network traffic or physical monitoring with cameras that are under their control. The persons responsible must be considered to be particularly trustworthy and reliable.
3.17	Trustworthy components may perform only the intended operations.
3.18	The software for the auditors' technical aids must be obtained from a different system developer from the one who developed the main part of the software for the other system components. The publication of the software for the technical aid under a licence that meets the criteria for open source software may justify an exception. If auditors use several technical aids, this provision applies to at least one of the technical aids.
3.19	All procedures for dealing with trustworthy components must be documented in writing and in a manner that is easily understood by the persons concerned.
3.20	Any access to and use of a trusted component or data carrier containing critical data must be logged.

Table 4 - E-voting requirements: Requirements for trustworthy components in accordance with Number 2 and their operation

Voting Process

Key	Requirement
4.1	The person voting must declare that he or she is aware of the rules on electronic voting and of his or her own responsibilities.
4.2	Before casting a vote, the person voting is notified that he or she is taking part in a ballot in the same way as voting by post or voting in person at the ballot box. The person voting may only cast his or her vote after confirming that he or she has taken note of this.
4.3	When voting, the person voting is requested to check the proofs in accordance with Number 2.5 against the verification reference and to report any doubts as to its correctness to the canton.
4.4	At any time before casting an electronic vote definitively, the voter may still choose to cast his or her vote via a conventional voting channel.
4.5	The client-side system as it appears to the person voting does not influence the person voting in his or her decision on how to vote.

Key	Requirement
4.6	The user guidance must not lead persons voting to cast hasty or ill-considered votes.
4.7	The system does not offer the person voting any functionality allowing them to print out or store their vote.
4.8	The person voting is not shown any information after the voting process is completed about the content of the vote that has been encrypted and cast.
4.9	A voter who is unable to cast a vote because third parties have cast a vote using his or her voting papers unlawfully may still be allowed to vote provided the canton declares the unlawfully cast vote null and void. Voting secrecy in accordance with Number 2.7 must be preserved.
4.10	Voters with disabilities may be provided with a simplified procedure for checking the proofs. Only in such a case are derogations from the requirements set out in Number 2.9.1 permitted.
4.11	As long as the system has not registered confirmation of a definitive electronic vote, the voter may still choose to cast his or her vote via a conventional voting channel.
4.12	The use of a means of authentication independent of electronic voting is permitted. Effects on the integrity of the verification of the right to vote and the preservation of voting secrecy must be examined in detail as part of the risk assessment.

Table 4 - E-voting requirements: Voting process

Preparation for the ballot

Key	Requirement
5.1	If the electoral register data is imported from a third-party system that is outside the canton's control, the data must be encrypted and signed. The signature must be verified on receipt of the data. For delivery to the printing office, the provisions of Number 7 take precedence.
5.2	The data required to examine the proofs in accordance with Number 2.6 must be handed over to the auditors.

Table 5 - E-voting requirements: Preparation for the ballot

Requirements for polling cards

Key	Requirement
6.1	If possible, the polling cards shall be designed so as to allow voters with a disability barrier-free access to electronic voting.
6.2	Security elements on the polling card (e.g., scratch codes) may only be used if there is a confirmation that the concealed information is well protected against unauthorised reading.
6.3	If it is decided not to use security elements to protect confidential information on the voting card, organisational procedures must be in place to ensure security.

Table 6 - E-voting requirements: Requirements for polling cards

Requirements for printing offices

Key	Requirement
7.1	The printing data used to produce the polling cards are transmitted encrypted and signed. Alternatively, a data carrier containing this data may be delivered in person. In this case, the data carrier must be transported and delivered to the printing office by two persons, who must both stay with the data carrier until it is delivered.
7.2	The encryption must meet the requirements of eCH standard 0014, Chapter 7.5. If encryption is symmetric, the secret decryption key is sent to the persons responsible at the printing office via a secure secondary channel.
7.3	The person responsible at the printing office who receives the data carrier must sign an acknowledgement of receipt.
7.8	The channel between the printing office and the voters may only be considered trustworthy if the bodies responsible under cantonal law deliver the packaged voting papers to the voters by post or ensure that it is handed over in person.

Table 7 - E-voting requirements: Requirements for printing offices

Information and instructions

Key	Requirement
8.1	The body responsible at cantonal level must issue guidelines on providing information to citizens about electronic voting.
8.2	The guidelines ensure that the information is authorised by the responsible bodies.
8.3	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.
8.4	Verifiability, further security measures and the procedure in the event of anomalies are explained to voters in an accessible manner.
8.5	Voters are told what they have to pay attention to in order to cast their vote securely.
8.6	Voters are given instructions on how to delete their vote from all the memories on the device used for entering the vote.
8.7	Voters may request support if they have questions about electronic voting.
8.8	Voters are requested to report incorrectly displayed proofs in accordance with Number 2.5 such as verification codes or other verification steps with negative results to the body responsible at cantonal level. This request is also made in the instructions sent out with the voting papers.
8.9	Voters are requested to keep the voting papers with the security elements in fulfilment of Number 2.5 securely until they cast their final vote or until the voting process is concluded.
8.10	Voters are given the information required to check the authenticity of the website and the server used for voting. The informative value of a successful check must be supported by the use of cryptographic resources according to the best practices.
8.11	The information essential for secure voting is sent with the voting papers. Voters are told that if in doubt, they should comply with the information in the voting papers rather than the information displayed on the user device.
8.12	The measures taken to preserve voting secrecy are explained to voters.
8.13	Known flaws and the need for action associated with them are communicated transparently.

Key	Requirement
8.14	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.

Table 8 - E-voting requirements: Information and instructions

Opening and closing the electronic voting channel

Key	Requirement
9	The electronic voting channel is only available during the permitted period.

Table 9 - E-voting requirements: Opening and closing the electronic voting channel

Tallying votes in the electronic ballot box

Key	Requirement
11.1	The decryption of the votes and the tallying may not begin before Polling Sunday.
11.2	The canton carries out the decryption and tallying within its own infrastructure.
11.3	The canton must ensure that the decryption of votes and their tallying is documented. The minutes are released by the body responsible at cantonal level.
11.4	From the decryption of votes to the transmission of the result of the ballot, any access to the system or to any of its components must be made jointly by at least two persons; it must be recorded in writing and it must be possible for the auditors to check it.
11.5	If the result data is transmitted to a third-party system that is outside the canton's control, the data must be encrypted and signed.
11.6	The system allows the polling card to be used to determine whether someone has cast an electronic vote.
11.7	Auditors must be present during decryption and tallying. The cantons may permit additional remote auditing work.
11.8	If components used to tally votes are not trustworthy in accordance with Number 2.4, the same requirements apply to these components as to set-up components under Number 3.
11.9	The auditors exercise their responsibility in accordance with cantonal law when examining the proofs in accordance with Number 2.6.
11.10	The body responsible at cantonal level submits all relevant indicators of the correctness of the result to the auditors. This includes, in addition to the proofs in accordance with Number 2.6, in particular the number and nature of anomalies reported to the canton by voters.
11.11	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.
11.12	Statistical methods must be used to check the plausibility of the result, provided they are available and there is sufficient data.

Table 10 - E-voting requirements: Tallying votes in the electronic ballot box

Confidential data

Key	Requirement
12.1	It is guaranteed that neither employees nor externals hold data that allow a connection to be made between the identity of persons voting and the votes they have cast.
12.2	It is guaranteed that neither employees nor externals hold data before the decryption of the votes that allow the premature determination of partial results.
12.3	The canton may not pass on to private companies its part of the key for decrypting the votes which it has on the control component that it operates in accordance with Number 3.1.
12.4	The canton must treat the results of the ballot as confidential between the time the votes are decrypted and the time of publication.
12.5	The canton must ensure that data that indicate whether a voter has voted electronically are treated as confidential.
12.6	The canton must treat the individual votes as confidential after they have been tallied.
12.7	The canton must ensure that vote and election results in small constituencies are treated as confidential.
12.8	Following validation and in accordance with a predetermined and documented process, all data created as part of the electronic ballot that relate to the individual votes received and that are classified as confidential must be destroyed.

Table 11 - E-voting requirements: Confidential data

Threats

<table>
<tr><th>Key</th><th colspan="3">Requirement</th></tr>
<tr><td>13.1</td><td colspan="3">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.</td></tr>
<tr><td>13.2</td><td colspan="3">The following are considered to be potential threats:
inadvertent or intended electronic or physical threats from internal or external actors;
threats resulting from a malfunction of the system or system-supporting elements

<table>
<tr><th></th><th>Description</th><th>Security objective concerned (in accordance with Art. 4 para. 3)</th></tr>
<tr><td>13.3</td><td>Malware changes the vote on the user device.</td><td>Accuracy of the result</td></tr>
<tr><td>13.4</td><td>An external attacker redirects the vote using domain name server spoofing (DNS spoofing)[2].</td><td>Accuracy of the result</td></tr>
</table>
</td></tr>
</table>

[2] Also known as DNS poisoning. This is an attack which successfully falsifies the correlation between a host name and the related IP address.

Key	Requirement		
	13.5	An external attacker changes vote using the man-in-the-middle (MITM) technique[3].	Accuracy of the result
	13.6	An external attacker sends a maliciously altered ballot paper using MITM.	Accuracy of the result
	13.7	An internal attacker manipulates the software, causing it not to store the votes.	Accuracy of the result
	13.8	An internal attacker changes the votes.	Accuracy of the result
	13.9	An internal attacker inserts votes.	Accuracy of the result
	13.10	A hostile organisation infiltrates the system with the aim of falsifying the result.	Accuracy of the result
	13.11	An internal attacker copies voting papers and uses them.	Accuracy of the result
	13.12	An external attacker uses social engineering techniques to distract the person voting from following the security measures (individual verifiability).	Accuracy of the result
	13.13	An external attacker infiltrates the canton's infrastructure electronically, physically or by means of social engineering and extracts security-relevant data while the parameters of the ballot are being set.	Accuracy of the result
	13.14	An external attacker infiltrates the printing office's infrastructure electronically, physically or by means of social engineering and extracts the codes of the polling cards.	Accuracy of the result
	13.15	An external attacker infiltrates the postal service's infrastructure electronically, physically or by means of social engineering and steals polling cards.	Accuracy of the result

[3] The attacker in a man-in-the-middle attack. This is a type of attack used in computer networks. The attacker is positioned either physically or logically between the two communication partners and via its system has full control of the data traffic between two or more network participants and can view or even manipulate any information it wants.

Key	Requirement		
	13.16	An error occurs in the individual verifiability.	Accuracy of the result
	13.17	An error occurs in the universal verifiability.	Accuracy of the result
	13.18	An error occurs in an auditor's technical aid.	Accuracy of the result
	13.19	A backdoor[4] is introduced into the system via a software dependency and is exploited by an external attacker to access the system.	Accuracy of the result, preservation of voting secrecy and exclusion of premature results, accessibility and operability of the voting system, protection of information intended for voters from manipulation, prevention of improper use of evidence of voting behaviour
	13.20	Malware on the user device sends the vote to a hostile organisation.	Preservation of voting secrecy and exclusion of premature results
	13.21	The vote is redirected using DNS spoofing.	Preservation of voting secrecy and exclusion of premature results
	13.22	An external attacker reads a vote using MITM.	Preservation of voting secrecy and exclusion of premature results
	13.23	An internal attacker uses the key and decrypts non-anonymous votes.	Preservation of voting secrecy and exclusion of premature results
	13.24	While checking the accuracy of the processing and tallying, voting secrecy is breached.	Preservation of voting secrecy and exclusion of premature results
	13.25	An internal attacker reads the votes at an early stage without having to decrypt the votes.	Preservation of voting secrecy and exclusion of premature results
	13.26	A hostile organisation infiltrates the system with the aim of breaching voting secrecy or obtaining premature results.	Preservation of voting secrecy and exclusion of premature results
	13.27	An error in the encryption process renders it inoperable or reduces its effectiveness.	Preservation of voting secrecy and exclusion of premature results
	13.28	Malware on the user device makes voting impossible.	Accessibility and operability of the voting system
	13.29	A hostile organisation carries out a denial-of-service (DOS)[5] attack.	Accessibility and operability of the voting system

[4] A backdoor is a portion of software that allows access to the computer or an otherwise protected function of a computer program by bypassing normal access protections.

[5] In digital data processing, this is the non-availability of a service that should be available.

Key	Requirement		
	13.30	An internal attacker carries out an incorrect configuration; it does not get to the tallying.	Accessibility and operability of the voting system
	13.31	An internal attacker falsifies the cryptographic proofs of universal verifiability.	Accessibility and operability of the voting system
	13.32	A technical error in the system causes the system to be unavailable at the time of the count.	Accessibility and operability of the voting system
	13.33	One of the auditors' technical aids does not work at the time of tallying.	Accessibility and operability of the voting system
	13.34	A hostile organisation infiltrates the system with the aim of disrupting operations, manipulating voter information or stealing proofs of the voting behaviour of the persons voting.	Accessibility and operability of the voting system, protection of information intended for voters from manipulation, prevention of improper use of evidence of voting behaviour
	13.35	An internal attacker steals voters' address data.	Protection of personal information relating to voters
	13.36	Malware influences voters' opinions.	Protection of information intended for voters from manipulation
	13.37	An internal attacker manipulates the information website or voting portal and thereby deceives voters.	Protection of information intended for voters from manipulation
	13.38	An internal attacker tells voters whether and how they have to vote. After decryption, he finds evidence in the infrastructure that the voters have followed the instructions.	Prevention of improper use of evidence of voting behaviour
	13.39	An external attacker tells voters whether and how they have to vote and demands evidence that they have followed the instructions.	Prevention of improper use of evidence of voting behaviour

Table 12 - E-voting requirements: Threats

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

Key	Requirement
14.1	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.

Key	Requirement
	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.
14.2	Records are created on the infrastructure whose recording, transmission and storage are resistant to manipulation (system logs). The records are consistent with each other and allow the relevant events to be traced when investigating suspected manipulation or errors. They serve as evidence of the complete, unfalsified and exclusive tallying of votes cast in conformity with the system, of preservation of voting secrecy and of the exclusion of premature partial results. The content of the records covers at least the following events: ■ start and end of the audit, identification and authentication processes; ■ start, restart and end of the voting or election phase; ■ start of the tallying with the determination of the results; ■ conduct and results of any self-tests; ■ malfunctions identified in elements of the IT infrastructure that affect the ability to operate. The date and time of each event, the type of event, the possible originator and the result in terms of failure or success are documented. The system logs are made available to the body responsible at cantonal level in such a way that it can interpret the information.
14.3	The monitoring and recording of system logs are subject to a continuous improvement process. The improvement process involves an open dialogue between those involved and a regular and objective assessment of the effectiveness of the instruments and processes used. The results of these evaluations will be taken into account.
14.4	The monitoring and recording of system logs in no way detracts from the effectiveness of the measures taken to preserve voting secrecy.
14.7	It is possible to cast control votes using authentication credentials that are not assigned to any voter. The content of these control votes is recorded. The tallying of the control votes is compared with the records. It must be ensured that the control votes are dealt with in as similar a way possible as votes cast in conformity with the system, while at the same time ensuring that they are not counted.
14.8	Infrastructure availability must be checked and recorded at selected intervals.
14.9	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.
14.10	The measures for monitoring and keeping records of system usage, the activities of administrators and of malfunction records must be described in detail, implemented, monitored and reviewed.

Table 13 - E-voting requirements: Identifying and reporting security events and vulnerabilities; dealing with security events and making security improvements

Use of cryptographic measures and key management

Key	Requirement
15.1	Electronic certificates must be managed according to the best practices.

Key	Requirement
15.2	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.
15.3	To ensure that critical data are kept secret, effective cryptographic measures are used in the infrastructure that correspond to the state of the art. Such data is always stored encrypted on data carriers.
15.4	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.

Table 14 - E-voting requirements: Use of cryptographic measures and key management

Secure electronic and physical exchange of information

Key	Requirement
16.1	All infrastructure components must be operated in a separate network zone. This network zone must be protected in relation to other networks by an appropriate routing control.
16.2	As a principle, electronic voting should be clearly separated from all other applications.

Table 15 - E-voting requirements: Secure electronic and physical exchange of information

Organisation of information security

Key	Requirement
18.1	All roles and responsibilities for the operation of the system must be precisely defined, assigned and communicated.
18.2	The initial configuration of the infrastructure, whether with regard to hardware, software or access rights, and any modification must be approved beforehand.
18.3	The risks in connection with third parties (contractors such as suppliers and service providers) must be identified and if necessary reduced by means of suitable contractual agreements. Compliance with the agreements must be appropriately monitored and reviewed throughout their term.

Table 16 - E-voting requirements: Organisation of information security

Management of intangible and tangible resources

Key	Requirement
19.1	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.
19.2	The acceptable use of intangible and tangible resources must be defined.
19.3	Classification guidelines for information must be issued and communicated.
19.4	Procedures must be devised for the labelling and handling of information.

Table 17 - E-voting requirements: Management of intangible and tangible resources

Trustworthiness of human resources

Key	Requirement
20.1	Suitable policies and procedures must be devised and promulgated in order to guarantee the trustworthiness of human resources before, during and after termination of employment or in the case of a change of activity.
20.2	Heads of human resources must accept full responsibility for guaranteeing the trustworthiness of human resources.
20.3	All human resources must be acutely aware of the significance of information security. To this end, an education and training programme that is tailored to the tasks concerned must be devised and operated.

Table 18 - E-voting requirements: Trustworthiness of human resources

Physical and environment security

Key	Requirement
21.1	The security perimeters of the various premises of the infrastructure are clearly defined.
21.2	For physical entry to these various infrastructure premises, entry controls must be defined, implemented and appropriately checked.
21.3	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.
21.4	All data must be processed and in particular stored exclusively in Switzerland.

Table 19 - E-voting requirements: Physical and environment security

Management of communication and operations

Key	Requirement
22.1	Obligations and areas of responsibility must be apportioned so that the risks originating from human resources relating to operations and communications are reduced to residual risks that are compatible with the risk acceptance criteria.

Key	Requirement
22.2	Appropriate measures must be taken to protect against malware.
22.3	A detailed plan for data backup must be prepared and implemented. The data backup must be regularly reviewed to check that it is functioning correctly.
22.4	Appropriate measures must be defined and implemented to protect the network from the threats listed in the risk assessment in accordance with Article 4 and in connection with Number 13 and for the security of network services.
22.5	The procedures for using removable data carriers and for disposing of data carriers must be regulated in detail.

Table 20 - E-voting requirements: Management of communication and operations

Allocation, administration and withdrawal of access and admission authorisations

Key	Requirement
23.1	It must be ensured that, during the ballot, any subsequent change in physical and logical access rights takes place only with the consent of the body responsible at cantonal level.
23.2	Access to infrastructure and software must be regulated and documented in detail on the basis of a risk assessment. In high-risk areas and for all manual operations in connection with the electronic ballot box (e.g. opening the voting channel, closing the voting channel, starting tallying), operations must be conducted by at least two persons. Manual operations in connection with the electronic ballot box (e.g. opening the voting channel, closing the voting channel, starting tallying) must be expressly authenticated.
23.3	It must be guaranteed that information on the voting portal and related information pages cannot be changed without authorisation.
23.4	During the ballot, access of any nature to the infrastructure that is of no relevance to the ballot must be prevented.
23.5	It must be ensured that none of the elements of the client-sided authentication credentials can be systematically intercepted, changed or redirected during transmission. For authentication, measures and technologies must be used that sufficiently minimise the risk of systematic abuse by third parties.

Table 21 - E-voting requirements: Allocation, administration and withdrawal of access and admission authorisations

Development and maintenance of information systems

Reliable and verifiable compilation and deployment

Key	Requirement
24.3.5	The quality of the evidence of reliable and verifiable compilation and reliable and verifiable deployment must be confirmed by the presence of at least two witnesses from different institutions or by technical procedures to establish the truth of the evidence in the light of current academic knowledge and experience.
24.3.6	The chain of evidence of reliable and verifiable compilation and deployment is made publicly available.

Table 22 - E-voting requirements: Reliable and verifiable compilation and deployment

Systematic correction of flaws

Key	Requirement
24.4.1	Processes are defined for the correction of flaws. The processes include: ■ documentation of specific aspects, in particular with regard to the traceability of flaws for all versions of the software, and of the methods used to ensure that system users have information on flaws, corrections and possible corrective actions; ■ the obligation to describe the nature and impact of all security flaws, information on the status of work to find a solution and the corrective measures adopted; ■ a description of how system users can make reports and enquiries about suspected flaws in the software known to the software developers; ■ a procedure requiring a timely response and automatic dispatch of security flaw reports and appropriate corrective actions to registered system users who may be affected by the flaw.

Table 23 - E-voting requirements: Systematic correction of flaws

Learnability

Key	Requirement
25.6.2	Persons who operate and use the system must be trained and provided with the necessary documentation.
25.6.3	Training includes the opportunity to train on a system designed for training purposes.
25.6.4	Help on using the system must be readily available.

Table 24 - E-voting requirements: Learnability

4 Examination results

22. This section enumerates the results of the examination for each item of the examination criteria.

Art 11

Key	Art.11
Requirement	**Art. 11 Disclosure of the source code and of the documentation on the system and its operation** 1 The canton shall ensure that the following documents are published: 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. 2 The following need not be published: 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	The Post has published most of the pieces of software used in the context of e-voting on its source code repository platform. During the setup phase, specific software is used to generate the polling cards in the form of PDF documents. The cantons of Basel-Stadt, Graubünden and Thurgau use the *VotingCardPrintService* (VPCS) from the Swiss Post. The software runs on a trusted component and manipulates critical data. The source of the software is not published. A set of scripts are also used by the cantons to simplify the operations that need to be carried out on the laptops. The source of these scripts is not published. Both the software used to create PDF files and the scripts do not fall under the exceptions of art. 11.2.a since these third-party components are not widely used but rather tools used only for the Swiss e-voting system. To ensure that that the machine-readable programmes were generated from the published software source code, the cantons perform a compilation of the source code and check the hash values of the corresponding binaries against values provided by the Post.
Evidence	■ https://gitlab.com/swisspost-evoting/e-voting/e-voting ■ https://github.com/abraxas-labs/voting-stimmunterlagen-offline-client-docs/ ■ E-Voting-System Post R. 1.4.4.4:Trusted-Build: Bericht

	■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 0.3.3
Result	Fail
Finding	The source code of the VPCS software, which is used to generate polling cards in Basel-Stadt, Graubünden, and Thurgau, as well as the source code of the associated helper scripts, has not been published. The publication of the VPCS software's source code is planned for May 2025.
Relevance	N/A

Table 25 – Examination results: OEV Art.11

Art 14

Key	Art.14
Requirement	**Responsibility for running the ballot with electronic voting correctly** 1 The canton bears overall responsibility for running the ballot with electronic voting correctly. 2 It must carry out important tasks itself. 3 It may delegate the development of the software used, technical operational tasks and communication on questions about how the system works to external organisations.
Observation	The *Konzept E-Voting* document lists the cantons' units involved in e-voting, as well as their areas of responsibilities. The cantons are responsible for the introduction, implementation and operation of e-voting, including: ■ Preparation of the ballots; ■ Generation, printing and packaging of the voting cards; ■ Provision of electronic ballot box; ■ Provision of digital instructions and voting guides; ■ Electronic voting of eligible voters (voting and election period); ■ Shuffling and decoding of the ballot box / counting; ■ Post-processing of the ballot box. The cantons rely on third parties for the development and operation of the e-voting software, the printing and packaging of the voting cards, some IT tasks performed on the laptops used to manage ballots (e.g. elaboration of the image), support on professional and technical issues. Those external organisations are listed in the *Konzept E-Voting* document.
Evidence	■ BS: E-Voting BS - Konzept E-Voting - V1.6, §2.2 ■ GR: E-Voting - Konzept E-Voting – V1.3, §3.2 ■ SG: E-Voting - Konzept E-Voting – V1.6, §3.2 ■ TG: E-Voting-TG-Konzept E-Voting – V1.6, §3.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 26 – Examination results: OEV Art. 14

Requirement for the cryptographic protocol: individual verifiability

Key	2.5
Requirement	The voter is given proofs in accordance with Article 5 paragraph 2 in conjunction with Article 6 letters a and b to confirm that no attacker ■ has altered any partial vote before the vote has been registered as cast in conformity with the system; ■ has maliciously cast a vote on the voter's behalf which has subsequently been registered as a vote cast in conformity with the system and counted.
Observation	The examiners assume that the properties depicted in Article 5 paragraph 2 in conjunction with Article 6 letters a and b (which are not part of the present audit scope) are met. When a vote has been submitted, and before it is confirmed, verification codes are displayed to the voter by the e-voting system. If identical to the codes on the voting material, they prove that partial votes have not been altered. If a voter logs in after a vote has been confirmed, the finalisation code is displayed. The absence of such code at login proves that no vote was cast maliciously.
Evidence	Demo Swiss Post voting Portal R1.4 (2025)
Result	Pass
Finding	N/A
Relevance	N/A

Table 27 – Examination results: OEV paragraph 2.5

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: ■ 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	The examiners assume that the properties depicted in Article 5 paragraph 3 letter a in conjunction with Article 6 letters a and c (which are not part of the present audit scope) are met. The document *Konzept Vollständige Verifizierbarkeit* specifies the technical means and the procedure to verify the correct processing of votes and the accuracy of the result of the electronic voting channel during a ballot. In step 3.4 of the *Prozesse E-Voting* document, the data necessary for verifying the proofs is extracted and provided to the auditors.
Evidence	■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 3.4 ■ BS, GR, SG, TG: E-Voting - Konzept Vollständige Verifizierbarkeit - V1.6, §4
Result	Pass

Finding	N/A
Relevance	N/A

Table 28 – Examination results: OEV paragraph 2.6

Requirements for the cryptographic protocol: preserving voting secrecy and excluding premature partial results

Key	2.7.1 & 2.7.2
Requirement	It must be ensured that no attacker is able to breach voting secrecy or establish premature partial results unless he can control the voters or their user devices (2.7.1). There is no obligation to prevent attacks that limit the number of tallied votes to the degree that all partial votes for a question, list or candidate are the same (2.7.2).
Observation	Maintaining voting secrecy and preventing the premature disclosure of a ballot's results are properties enforced through the implementation of a cryptographic protocol within the e-voting application amongst others. The Post has conducted a security analysis of the said cryptographic protocol to demonstrate it meets the intended security requirements when the user device is considered trustworthy and if at least one control component can be trusted. From the cantons' perspective, attack scenarios leading to a breach of voting secrecy or the possibility to establish premature results have been subject to a comprehensive risk analysis. They include: ■ Intentional or accidental compromising of the secrets necessary to decrypt the votes (decryption key, passwords protecting the decryption key), ■ Intentional or accidental disclosure of a ballot's results by a member of the admin- or the electoral- boards, ■ Presence of a malware on the voting portal allowing to send votes to a malicious third party, ■ Technical issue allowing to read the votes without decryption. The risk level for those threats is assessed as acceptable according to the risk analysis.
Evidence	■ Risk portfolio ● P07-R01 – Beide Passwörter sind einer Person bekannt ● P10-R01 – Verletzung des Stimmgeheimnisses ● P10-R02 – Stimmen werden an Dritte geschickt / von Dritten gelesen ● P10-R07 – Stimmen können ohne Entschlüsselung gelesen werden ● P12-R02 – Vorzeitige Offenlegung der EV-Ergebnisse
Result	Pass
Finding	N/A
Relevance	N/A

Table 29 – Examination results: OEV paragraph 2.7.1& 2.7.2

Key	2.7.3

Requirement	It must be ensured that no attacker can take control of user devices unnoticed by manipulating the user device software on the server. The person voting must be able to verify that the server has provided his or her user device with the correct software with the correct parameters, in particular the public key for encrypting the vote.
Observation	The voting client application (more precisely, the *GetKey* algorithm) checks that the public key used to encrypt votes submitted by the persons voting corresponds to the key that was created by the cantons in the election setup component. An error message is triggered if it is not the case. The algorithm also checks the other input and context arguments from the voting server. The values are checked using the start voting key (SVK), which is printed on the voting card and entered by the voting person. The voting client application is composed of a HTML file (*index.html)* and JavaScript files. The integrity of the JavaScript files can be checked by the voting persons thanks to the use of the *subresource integrity* tag, a functionality that compares the hash value of the served files with the genuine hash values made available in the protocols published by the cantons. The procedure is described in the Post's e-voting documentation. The e-voting documentation also provides instructions to verify the integrity of the *index.html* file manually and to control the fingerprint of the voting portal's TLS certificate.
Evidence	■ Swiss Post Voting System - System specification v1.4.1.1 ■ https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/Security-advices/en/readme.md ■ E-voting demo website: https://demo.evoting.ch/
Result	Pass
Relevance	N/A

Table 30 – Examination results: OEV paragraph 2.7.3

Requirement for the cryptographic protocol: effective authentication

Key	2.8
Requirement	It must be ensured that no attacker can cast a vote in conformity with the system without having control over the voters concerned.
Observation	The cryptographic protocol ensures that votes can only be cast using the codes printed on the voting cards. To cast a vote in conformity with the system without having control over the voters, an attacker should therefore gain access to those codes. The cantons participate to the creation of the codes during the setup phase and send them to the printing office for printing and postal delivery to the voters. The following security measures are applied to protect their confidentiality: ■ All operations in connection with the setup phase are subject to the 4-eye principle, ■ The codes are generated on an off-line machine, ■ The data sent by the cantons to the printing office is encrypted and signed.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, §3.2, 3.4
Result	Pass
Finding	N/A

Relevance	N/A

Table 31 – Examination results: OEV paragraph 2.

For soundness of the proofs referred to in Number 2.5

	2.9.1.2
	The following system participants may be considered trustworthy: ■ set-up component ■ print component ■ one of four control components per group, leaving open which one it is
	This requirement is taken into account when auditing requirements about trustworthy components (See Number 3.1-3.20).
	N/A
	N/A
	N/A
	N/A

Table 32 – Examination results: OEV paragraph 2.9.1.2

For soundness of the proofs referred to in Number 2.6

Key	2.9.2.2
Requirement	The following system participants may be considered trustworthy: ■ one of four control components per group, leaving open which one it is ■ one auditor in any group, leaving open which auditor it is ■ one technical aid from a trustworthy auditor, leaving open which aid it is
Observation	This requirement is taken into account when auditing requirements about trustworthy components.
Evidence	N/A
Result	N/A
Finding	N/A
Relevance	N/A

Table 33 – Examination results: OEV paragraph 2.9.2.2

For preserving voting secrecy and excluding premature partial results in accordance with Number 2.7

Key	2.9.3.2
Requirement	The following system participants may be considered trustworthy: ■ set-up component ■ print component ■ user device ■ one of four control components per group, leaving open which one it is

Observation	This requirement is taken into account when auditing requirements about trustworthy components (See Numbers 3.1-3.20).
Evidence	N/A
Result	N/A
Finding	N/A
Relevance	N/A

Table 34 – Examination results: OEV paragraph 2.9.3.2

Requirements for the definition and description of the cryptographic protocol

Key	2.13.3
Requirement	It may be assumed that trustworthy channels exist to distribute electronic certificates among system participants. Number 3.8 applies.
Observation	This requirement is taken into account when auditing requirements about the distribution of certificates (See Numbers 3.8, 15.1).
Evidence	N/A
Result	N/A
Finding	N/A
Relevance	N/A

Table 35 – Examination results: OEV paragraph 2.1.3.3

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

	3.1
	The operation of the set-up component and at least one control component in the group which contains part of the key for decrypting the votes is the direct responsibility of the canton and must take place within its infrastructure. Outsourcing to a private system operator is not permitted.
	The cantons assume the responsibility for the set-up component (a.k.a. *setup computer)* and the control component (a.k.a. *tally computer*) containing part of the key for decrypting the votes. They operate these components within their own infrastructure.
	BS: E-Voting BS Konzept E-Voting - V1.6, §2.3 GR: E-Voting - Konzept E-Voting - V1.3, §3.3 SG: E-Voting - Konzept E-Voting - V1.6, §3.3 TG: E-Voting-TG-Konzept E-Voting - V1.6, §3.3
	Pass
	N/A
	N/A

Table 36 – Examination results: OEV paragraph 3.1

Key	3.2
Requirement	Sufficient entropy must be ensured when selecting random values, in particular for set-up components and control components.
Observation	Most random values in the setup component and the control component are generated by the software obtained from the Post. Analysis of this software is performed within the audit scope: *2 e) Assess the implementation of the protocol*. In some cases, the operators of the setup component must choose random passwords of a certain length (e.g., for the encryption of the printing files, for setting up the electoral board, for the e-voting laptops' passwords). The *Richtlinie Informationssicherheit* document sets the requirements in terms of password length, so that sufficient entropy is ensured.
Evidence	BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.3 GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.3 SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.3 TG: E-Voting-TG-Richtlinie Informationssicherheit – V1.3, §4.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 37 – Examination results: OEV paragraph 3.2

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	The document *E-Voting - Konzept Vollständige Verifizierbarkeit* mentions the proofs verification as part of the auditors' duties and details the tasks to be performed. In step 3.4 of *Prozesse E-Voting* the auditors use the technical aid to verify the proofs.
Evidence	■ BS, GR, SG, TG: E-Voting - Konzept Vollständige Verifizierbarkeit - V1.6, §3.3, §4 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 3.4
Result	Pass
Finding	N/A
Relevance	N/A

Table 38 – Examination results: OEV paragraph 3.3

Key	3.4
Requirement	The operational requirements for set-up components in accordance with Number 3 also apply to technical aids used by the auditors. Within the scope of their responsibility under cantonal law, the auditors may provide for derogations.
Observation	According to Art. 5 of the OEV, technical aids are the tools used to prove that the requirements for universal verifiability are met during the voting process.

Evidence	The cantons provide a laptop containing the technical aid (i.e. the *Verifier*). This laptop is set up and operated in the same way as the other trustworthy components.
	■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §4 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §5 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §5 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §5 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, steps 0.3.1, 0.3.4, 0.5, 2.6, 3.4
Result	Pass
Finding	N/A
Relevance	N/A

Table 39 – Examination results: OEV paragraph 3.4

Key	3.5
Requirement	With the exception of the components mentioned under Numbers 3.1 and 3.3, the canton may delegate the operation of any part of the system, including the control components and the print component, to private service providers. A private operator of the print component may only perform operational tasks that are required for preparation, packaging and delivery.
Observation	Four control components are operated by the Swiss Post, one by the cantons. The voting material is printed by specialised external third parties, that only perform operational tasks required for preparation, packaging and delivery.
Evidence	■ Swiss Post E-Voting Architecture Document v1.4.0, §5.5, 5.6 ■ BS: E-Voting BS - Konzept E-Voting - V1.6, §5.4 ■ GR: E-Voting - Konzept E-Voting – V1.3, §6.7 ■ SG: E-Voting - Konzept E-Voting – V1.6, §6.4 ■ TG: E-Voting-TG-Konzept E-Voting – V1.6, §6.6
Result	Pass
	N/A
	N/A

Table 40 – Examination results: OEV paragraph 3.5

Key	3.6
Requirement	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.
Observation	The installation, configuration and update of the trustworthy components is performed either by the cantons' IT team members or by an IT supplier, following a defined procedure. The process is observable as all operations are performed in respect of the 4-eye principle.
Evidence	■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §4 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §5 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §5 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §5

Result	Pass
Finding	N/A
Relevance	N/A

Table 41 – Examination results: OEV paragraph 3.6

Key	3.7
Requirement	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.
Observation	The *Prozesse E-Voting* document includes verifying the hash values of the software delivered by the Post as a task to perform. The *Hardware und Infrastruktur* document specifies that all the software is procured from official sources. The installation process includes verifying the hash value or the signature of the binaries, as well as an antivirus scan.
Evidence	■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §4 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §5 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §5 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §5 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 0.3.4
Result	Pass
Finding	N/A
Relevance	N/A

Table 42 – Examination results: OEV paragraph 3.7

Key	3.8
Requirement	When other system participants' electronic certificates are installed, their authenticity must be ensured. To that end, there should be a manual process in which people transfer the electronic certificates from one machine to another via a physical data carrier in accordance with 3.13.
Observation	The certificates are distributed through an electronic channel. The fingerprints are exchanged via a different channel and the correct transmission of the fingerprint is verified person-to-person in a physical or online meeting.
Evidence	BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.3 GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.3 SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.3 TG: E-Voting-TG-Richtlinie Informationssicherheit – V1.6, §4.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 43 – Examination results: OEV paragraph 3.8

Key	3.9

Requirement	The timing for updating all software of trustworthy components must be such that the expected benefits outweigh the potential hazards.
Observation	All software on trustworthy components is updated during the preparation phase of a vote. The Post's general instruction is to install the newest version of the software on the trustworthy components. The Post monitors the publication of vulnerabilities affecting the software and alerts the cantons when such a case occurs. A risk-based decision involving the cantons is taken.
Evidence	■ BS, GR, SG, TG: E-Voting – Basic installation and hardening – V1.7 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 0.3.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 44 – Examination results: OEV paragraph 3.9

Key	3.10
Requirement	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.
Observation	The e-voting components involved in the processing of critical data are subject to physical monitoring by the members of the Admin-Board during the whole computing time.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8
Result	Pass
Finding	N/A
Relevance	N/A

Table 45 – Examination results: OEV paragraph 3.10

Key	3.11
Requirement	Trustworthy components may not be connected to the internet when installing or updating software.
Observation	The trustworthy components are set up from a removable medium, without any connection to the internet.
Evidence	■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §4 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §5 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §5 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §5
Result	Pass
Finding	N/A

Relevance	N/A

Table 46 – Examination results: OEV paragraph 3.11

Key	3.12
Requirement	In principle, critical data must be destroyed after use. If there are good reasons, secure storage of the data carrier is also permitted as an alternative.
Observation	The cantons do not delete any data from the e-voting components until the preservation period (*Erwahrungsfrist*) is over (i.e. the vote has been validated) the laptops and the removable storage media are kept in safes in case a forensic analysis must be carried out. This is considered a valid reason according to requirement 3.12. If a new election has to be prepared before the validation, data on laptops and removable storage media is deleted and only the backup memory stick is kept in the safe.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, §4.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 47 – Examination results: OEV paragraph 3.12

Key	3.13
Requirement	Data exchange or storage media, such as USB flash drives, must be removed after the data has been uploaded to the trustworthy components and may only be reused before the data is destroyed if there was no critical data on the trustworthy component before the data was uploaded. Data exchange or storage media must be reformatted and any data on them must be destroyed before they are used with the aid of a component operated in accordance with the requirements for trustworthy components.
Observation	The data stored on the USB flash drives used in the context of e-voting events is deleted (using the *sDelete* tool) and the drives are reformatted during the preparation phase of a voting event. The cantons provision a sufficient number of drives to make a unique use of each of them during an event. This ensures that no data persists on the drives when those are reused.
Evidence	■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §3.2 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §4.2 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §4.2 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §4.2 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 0.3.3, §4.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 48 – Examination results: OEV paragraph 3.13

Key	3.14
Requirement	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).
Observation	The *Richtlinie Informationssicherheit* document mentions that all manual operations related to the electronic ballot box are subject to the 4-eye principle, including the access to and use of trustworthy components or data carriers. Such accesses are logged. The trustworthy components and data carriers are stored in a safe, whose access code is split into two parts to enforce the two-person principle.
Evidence	■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §6 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §7 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §7 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §7 ■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.4, 3.6, 3.7 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.4, 4.6, 4.7 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.4, 4.6, 4.7 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4.4, 4.6, 4.7
Result	Pass
Finding	N/A
Relevance	N/A

Table 49 – Examination results: OEV paragraph 3.14

Key	3.15
Requirement	Success in gaining unauthorised access to a control component should not as far as possible give any advantage in an attempt to access another control component unnoticed. In addition to the requirements set out in Number 3, the following requirements apply in this respect: ■ If a person has physical or logical access to a control component, that person may not have access to any other control component. ■ The hardware, the operating systems and the monitoring systems for the control components should be as distinct as possible from each other. ■ The control components should be connected to different local networks. ■ A control component must take the form of a physical device. Virtualisation across multiple physical devices is not permitted.
Observation	The cantons physically host one of the e-voting system's control components (a.k.a. the *tally computer*), in an offline-mode, whereas the other control components are hosted in the Post's premises. Therefore, gaining unauthorised access to the control component hosted by the cantons does not provide any advantage to access another control components. The cantons' representatives having physical or logical access to the local control component have no access to the other control components, which are accessed solely by the Post's employees. The cantons' representatives monitor their local control component, whereas the other control components are monitored by the Post's employees.

Evidence	The control components operated by the cantons run on dedicated hardware (i.e. a laptop procured directly by the cantons) and on the Windows 10 operating system; the control components operated by the Post run on physical servers, three of them on Linux distributions, the last one on Windows.
	■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §3.1 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §4.1 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §4.1 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §5 ■ BS, GR, SG, TG: E-Voting - Basic installation and hardening - V1.7
Result	Pass
Finding	N/A
	N/A

Table 50 – Examination results: OEV paragraph 3.15

Key	3.16
Requirement	Control components must be designed to recognise unpermitted instances of access and to alert the persons responsible. The persons responsible should arrange external monitoring measures, such as the monitoring and the manipulation-resistant logging of network traffic or physical monitoring with cameras that are under their control. The persons responsible must be considered to be particularly trustworthy and reliable.
Observation	The cantons' control component is off-line and can only be accessed physically. There are always at least two people watching the control component when it is not locked in a safe. These persons are subject to the requirements set in Number 20: *Trustworthiness of human resources*.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8
Result	Pass
Finding	N/A
Relevance	N/A

Table 51 – Examination results: OEV paragraph 3.16

Key	3.17
Requirement	Trustworthy components may perform only the intended operations.
Observation	The cantons apply strict hardening measures (e.g. deinstallation of unneeded software, deactivation of unneeded services, interfaces, application of secure configurations, etc.) on trustworthy components in order to limit their use to intended operations only.
Evidence	■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §4.1.3 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §5.1.3 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §5.1.3 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §5.1.3 ■ BS, GR, SG, TG: E-Voting – Basic installation and hardening – V1.7
Result	Pass
Finding	N/A

Relevance	N/A

Table 52 – Examination results: OEV paragraph 3.17

Key	3.18
Requirement	The software for the auditors' technical aids must be obtained from a different system developer from the one who developed the main part of the software for the other system components. The publication of the software for the technical aid under a licence that meets the criteria for open source software may justify an exception. If auditors use several technical aids, this provision applies to at least one of the technical aids.
Observation	The software for the auditors' technical aid (i.e. the V*erifier*) is provided by the same system developer as the one who developed the main parts of the e-voting system, but it has been published as an open source software.
Evidence	■ BS, GR, SG, TG: E-Voting - Konzept Vollständige Verifizierbarkeit - V1.6, §4.1 ■ https://gitlab.com/swisspost-evoting/verifier/verifier
Result	Pass
Finding	N/A
Relevance	N/A

Table 53 – Examination results: OEV paragraph 3.18

Key	3.19
Requirement	All procedures for dealing with trustworthy components must be documented in writing and in a manner that is easily understood by the persons concerned.
Observation	The *Prozesse E-Voting* document presents the procedures for dealing with the trustworthy components in tables, which allows an easy understanding of the said procedures by the persons concerned.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8
Result	Pass
Finding	N/A
Relevance	N/A

Table 54 – Examination results: OEV paragraph 3.19

Key	3.20
Requirement	Any access to and use of a trusted component or data carrier containing critical data must be logged.
Observation	The cantons log the operations performed during the preparation and in the course of a ballot (i.e. the periods during which critical data is processed), as described in the *Prozesse E-Voting* document. They sign a generic report confirming that the processes were followed and attach a copy of the operational guide that was followed. Any deviation from the standard process is explicitly logged.
Evidence	E-Voting - Prozesse E-Voting - V1.8, §4.4

Result	Pass
Finding	N/A
Relevance	N/A

Table 55 – Examination results: OEV paragraph 3.20

Voting process

Key	4.1
Requirement	The person voting must declare that he or she is aware of the rules on electronic voting and of his or her own responsibilities.
Observation	The e-voting portal's landing page includes legal provisions of which users must confirm that they are aware before accessing the actual voting pages.
Evidence	Swiss Post demo voting Portal (https://demo.evoting.ch/vote/#/legal-terms/7E5EF56D52216DD9AEA47EBA78F6C6E8)
Result	Pass
Finding	N/A
Relevance	N/A

Table 56 – Examination results: OEV paragraph 4.1

Key	4.2
Requirement	Before casting a vote, the person voting is notified that he or she is taking part in a ballot in the same way as voting by post or voting in person at the ballot box. The person voting may only cast his or her vote after confirming that he or she has taken note of this.
Observation	The e-voting portal displays a notification stating that after the submission of his/her vote, the voting person will not be able to vote per post or in person.
Evidence	Swiss Post demo voting Portal
Result	Pass
Finding	N/A
Relevance	N/A

Table 57 – Examination results: OEV paragraph 4.2

Key	4.3
Requirement	When voting, the person voting is requested to check the proofs in accordance with Number 2.5 against the verification reference and to report any doubts as to its correctness to the canton.
Observation	Once the vote has been cast, the e-voting portal displays verification codes, which should match the values printed on the voting card. The voting person is invited to contact the cantonal authorities in case the values do not match.
Evidence	■ Swiss Post demo voting Portal

	■ Test polling card
Result	Pass
Finding	N/A
Relevance	N/A

Table 58 – Examination results: OEV paragraph 4.3

Key	4.4
Requirement	At any time before casting an electronic vote definitively, the voter may still choose to cast his or her vote via a conventional voting channel.
Observation	The voting system only blocks the conventional channels once the voter has confirmed the vote by submitting the confirmation code. Thus, it is possible to abort an ongoing electronic voting process at any time and take a conventional voting channel.
Evidence	Swiss Post demo voting Portal
Result	Pass
Finding	N/A
Relevance	N/A

Table 59 – Examination results: OEV paragraph 4.4

Key	4.5
Requirement	The client-side system as it appears to the person voting does not influence the person voting in his or her decision on how to vote.
Observation	The appearance of the voting system is simple and lists all voting options in the same way, which in the examiners' opinion, allows not to influence the person voting in his/her choice.
Evidence	Swiss Post demo voting Portal
Result	Pass
Finding	N/A
Relevance	N/A

Table 60 – Examination results: OEV paragraph 4.5

Key	4.6
Requirement	The user guidance must not lead persons voting to cast hasty or ill-considered votes.

Observation	The cantons have developed a communication concept for the voting persons, whose general objective is to "ensure that voters receive all the necessary information and assistance to cast their vote safely". It includes guidance regarding the voting process itself, directly available on the voting portal, as well as information on procedural security measures: handling of security codes, instructions on how to proceed in the event of anomalies (e.g. call to contact helpdesk and abort the electronic voting process in the event of incorrectly displayed verification codes). This information related to security procedures is made available on several media (cantons' website, e-voting information platform, voting portal, voting material). During the voting process, there is an explicit step for confirming a vote and a message is displayed, warning that the vote cannot be modified afterwards. Given the communication efforts made, the examiners estimate that the user guidance does not lead persons voting to cast hasty or ill-considered votes.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §3, 5 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §4, 6 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §4, 6 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §4, 6
Result	Pass
Finding	N/A
Relevance	N/A

Table 61 – Examination results: OEV paragraph 4.6

Key	4.7
Requirement	The system does not offer the person voting any functionality allowing them to print out or store their vote.
Observation	The e-voting system does not support a print nor a store function.
Evidence	Swiss Post demo voting Portal
Result	Pass
Finding	N/A
Relevance	N/A

Table 62 – Examination results: OEV paragraph 4.7

Key	4.8
Requirement	The person voting is not shown any information after the voting process is completed about the content of the vote that has been encrypted and cast.
Observation	The e-voting system's design meets this requirement.
Evidence	Swiss Post demo voting Portal
Result	Pass
Finding	N/A
Relevance	N/A

Table 63 – Examination results: OEV paragraph 4.8

Key	4.9
Requirement	A voter who is unable to cast a vote because third parties have cast a vote using his or her voting papers unlawfully may still be allowed to vote provided the canton declares the unlawfully cast vote null and void. Voting secrecy in accordance with Number 2.7 must be preserved.
Observation	According to the *Teilrevision der Verordnung über die politischen Rechte und Totalrevision der Verordnung der BK über die elektronische Stimmabgabe (Neuausrichtung des Versuchsbetriebs)- Erläuterungen zum Inkrafttreten vom 01. Juli 2022* document, the cantons are authorised to provide this functionality, but are not obliged to. The cantons have chosen not to provide it.
Evidence	N/A
Result	Pass
Finding	N/A
Relevance	N/A

Table 64 – Examination results: OEV paragraph 4.9

Key	4.10
Requirement	Voters with disabilities may be provided with a simplified procedure for checking the proofs. Only in such a case are derogations from the requirements set out in Number 2.9.1 permitted.
Observation	The cantons of Graubünden and St.Gallen have designed their voting cards so that the codes be machine-readable, which allows visually impaired people to vote electronically.
Evidence	N/A
Result	Pass
Finding	N/A
Relevance	N/A

Table 65 – Examination results: OEV paragraph 4.10

Key	4.11
Requirement	As long as the system has not registered confirmation of a definitive electronic vote, the voter may still choose to cast his or her vote via a conventional voting channel.
Observation	The voting system only blocks the conventional channels once the voter has confirmed the vote by submitting the confirmation code. If, for any reason, the system does not register confirmation of an electronic vote, voters have the possibility to opt for a conventional voting channel.
Evidence	Swiss Post demo voting Portal
Result	Pass
Finding	N/A
Relevance	N/A

Table 66 – Examination results: OEV paragraph 4.11

Key	4.12
Requirement	The use of a means of authentication independent of electronic voting is permitted. Effects on the integrity of the verification of the right to vote and the preservation of voting secrecy must be examined in detail as part of the risk assessment.
Observation	The cantons currently do not use means of authentication independent of electronic voting. This requirement therefore does not apply to it.
Evidence	Interviews
Result	Pass
Finding	N/A
Relevance	N/A

Table 67 – Examination results: OEV paragraph 4.12

Preparations for the ballot

Key	5.1
Requirement	If the electoral register data is imported from a third-party system that is outside the cantons' control, the data must be encrypted and signed. The signature must be verified on receipt of the data. For delivery to the printing office, the provisions of Number 7 take precedence.
Observation	The cantons only import electoral register data from cantonal systems, thus the requirement does not apply.
Evidence	■ BS: E-Voting BS - Konzept E-Voting - V1.6, §7.2.1 ■ GR: E-Voting - Konzept E-Voting – V1.3, §8.2.1 ■ SG: E-Voting - Konzept E-Voting – V1.6, §8.2.1 ■ TG: E-Voting-TG-Konzept E-Voting – V1.6, §8.2.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 68 – Examination results: OEV paragraph 5.1

Key	5.2
Requirement	The data required to examine the proofs in accordance with Number 2.6 must be handed over to the auditors.
Observation	In steps 3.4.1 – 3.4.2 of the *Prozesse E-Voting* document, the data necessary for verifying the proofs is extracted and provided to the auditors. The document *Konzept Vollständige Verifizierbarkeit* explains how this data is handled to attest that the ballot conforms to the requirements set in Number 2.6.
Evidence	■ BS, GR, SG, TG: E-Voting - Konzept Vollständige Verifizierbarkeit - V1.6, §4 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, steps 3.4.1, 3.4.2

Result	Pass
Finding	N/A
Relevance	N/A

Table 69 – Examination results: OEV paragraph 5.2

Requirements for polling cards

Key	6.1
Requirement	If possible, the polling cards shall be designed so as to allow voters with a disability barrier-free access to electronic voting.
Observation	In the cantons of Basel-Stadt and Graubünden, the polling cards have been designed in order to optimise automatic reading by a computer. This allows visually impaired persons to vote electronically. The cantons of St. Gallen and Thurgau have not taken any specific action to allow voters with a disability barrier-free access to electronic voting at this stage. However, such action is only recommended, not a must.
Evidence	Interviews
Result	Pass
Finding	N/A
Relevance	N/A

Table 70 – Examination results: OEV paragraph 6.1

Key	6.2
Requirement	Security elements on the polling card (e.g., scratch codes) may only be used if there is a confirmation that the concealed information is well protected against unauthorised reading.
Observation	The polling cards used by the cantons do not contain security elements. This requirement is therefore not applicable.
Evidence	Interviews
Result	Pass
Finding	N/A
Relevance	N/A

Table 71 – Examination results: OEV paragraph 6.2

Key	6.3
Requirement	If it is decided not to use security elements to protect confidential information on the voting card, organisational procedures must be in place to ensure security.

Observation	Security elements are one way of detecting an attempt to use a voting card both for electronic voting and physical voting. To vote electronically, the security element must be broken to reveal the start voting code. This alteration of the card can be detected if there is an attempt to reuse it via mail or at a booth. The audited systems do not use a security element. Instead, when the voting person uses a conventional voting channel, an online lookup is performed on each voting channel to confirm that the same card has not been used already. The cantons of Graubünden and Thurgau issue voting cards that are only valid for the electronic vote. Reusing the voting card to vote via mail or at a booth is not possible.
Evidence	■ BS: E-Voting BS - Konzept E-Voting - V1.6, §5.5 ■ GR: E-Voting - Konzept E-Voting – V1.3, §6.3, 6.4 ■ SG: E-Voting - Konzept E-Voting – V1.6, §6.5 ■ TG: E-Voting-TG-Konzept E-Voting – V1.6, §6.3, 6.7
Result	Pass
Finding	N/A
Relevance	N/A

Table 72 – Examination results: OEV paragraph 6.3

Requirements for printing offices

Key	7.1
Requirement	The printing data used to produce the polling cards are transmitted encrypted and signed. Alternatively, a data carrier containing this data may be delivered in person. In this case, the data carrier must be transported and delivered to the printing office by two persons, who must both stay with the data carrier until it is delivered.
Observation	The cantons of Basel Stadt, Graubünden and Thurgau use the *Voting Card Print Service (VCPS)* to generate, and sign the polling cards, and the *AxCrypt* software to encrypt the data. (*AxCrypt* is scheduled to be replaced by a proprietary software developed by the Post: *File-Cryptor*). The canton of St. Gallen uses the *VOTING Stimmunterlagen Offline* software provided by the Abraxas print office to generate, sign and encrypt the polling cards. The transmission of the data to the Abraxas print office occurs via a secure transfer platform operated by the cantons. In Basel-Stadt, Graubünden, and Thurgau, the decrypting password is sent to a different person than the one that received the data, via an alternative channel (i.e., the *Threema* secure messaging system). The *VOTING Stimmunterlagen Offline* software provides an asymmetric encryption mechanism. Therefore, no password needs to be transmitted to the Abraxas print office by the canton of St. Gallen. The cantons of Basel-Stadt and Thurgau also work with the Baumer print office for the printing of the polling cards. The canton of Basel-Stadt transmits the data via it secure transfer platform. The canton of Thurgau delivers the print data in person using a physical storage medium and in respect of the 4-eye principle.
Evidence	■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, steps 1.11, SRA-1 ■ BS. GR, TG: Benutzeranleitung (OG Post) Release 1.4 v11, §4.7.2, 4.7.4 ■ SG: Benutzeranleitung (OG Post) Release 1.4 v11, §9.3.2 ■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas – V1.1, §2.2

	■ BS: E-Voting BS - Prozessbeschreibung für die Produktion von E-voting-Stimmrechtsausweisen_Baumer - V2.0_unterzeichnet, §3.3 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.0 §2.3 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1, §2.3 ■ TG: E-Voting-TG-Prozessbeschreibung-für-die-Produktion-von-E-Voting-Stimmrechtsausweisen-Baumer-V2.0, §3.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 73 – Examination results: OEV paragraph 7.1

Key	7.2
Requirement	The encryption must meet the requirements of eCH standard 0014, Chapter 7.5. If encryption is symmetric, the secret decryption key is sent to the persons responsible at the printing office via a secure secondary channel.
Observation	The eCH standard 0014, §7.5 lists the recommended cryptographic algorithms to be used by Swiss e-government applications. The *E-Voting – Richtlinie Informationssicherheit* document includes a paragraph on the use of cryptography, which states that the algorithms used in the context of e-voting must conform to the eCH standard 0014. The Post's operational guide details the algorithms used to sign the print data using the *Voting Card Print Service (VCPS)* software (RSASSA-PSS algorithm, SHA-256 hash) and encrypt them using the *AxCrypt* software (AES-128). The decrypting key for files encrypted using *AxCrypt* is sent via the *Threema* mobile application. *File-Cryptor*, the software developed by the Post to replace *AxCrypt* relies on AES-256.
Evidence	■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step SRA-1 ■ BS, GR, TG: Benutzeranleitung (OG Post) Release 1.4 v11, §4.7.2, 4.7.4 ■ SG: VOTING_Stimmunterlagen_Offline_User_Manual_V0.92_Entwurf, §3.7 ■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.3 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.3 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.3 ■ TG: E-Voting-TG-Richtlinie Informationssicherheit – V1.6, §4.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 74 – Examination results: OEV paragraph 7.2

Key	7.3
Requirement	The person responsible at the printing office who receives the data carrier must sign an acknowledgement of receipt.

Observation	The *Prozesse E-Voting* document mentions that the print office signs a delivery note to acknowledge receipt of the printing data.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step SRA-1
Result	Pass
Finding	N/A
Relevance	N/A

Table 75 – Examination results: OEV paragraph 7.3

Key	7.8
Requirement	The channel between the printing office and the voters may only be considered trustworthy if the bodies responsible under cantonal law deliver the packaged voting papers to the voters by post or ensure that it is handed over in person.
Observation	The *Prozesse E-Voting* document mentions that the print office hands over the envelopes to the post office on behalf of the cantons at the agreed date for dispatch.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step SRA-3
Result	Pass
Finding	N/A
Relevance	N/A

Table 76 – Examination results: OEV paragraph 7.8

Information and instructions

Key	8.1
Requirement	The body responsible at cantonal level must issue guidelines on providing information to citizens about electronic voting.
Observation	The *Konzept Information der Stimmberechtigten* document details the types of information provided by the cantons' State Chancellery to citizens and specifies the associated communication channels
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5 §3, 5 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3 §4, 6 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5 §4, 6 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5 §4, 6
Result	Pass
Finding	N/A
Relevance	N/A

Table 77 – Examination results: OEV paragraph 8.1

Key	8.2
Requirement	The guidelines ensure that the information is authorised by the responsible bodies.

Observation	The guidelines specify that providing information to citizens about electronic voting, as well as the corresponding communication artefacts, are coordinated by and the responsibility of the head of e-voting.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §2 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §3 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §3 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §3
Result	Pass
Finding	N/A
Relevance	N/A

Table 78 – Examination results: OEV paragraph 8.2

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	The *Konzept Information der Stimmberechtigten* document mentions the kind of information provided regarding the electronic voting by communication channel. Communication over the internet includes the following media: the cantons' website, the information platform dedicated to e-voting, as well as the e-voting landing page itself. Tips and instructions to be provided include: ■ Information on e-voting security procedures (handling of the security codes), ■ Security advice with regards to technical security measures and on controlling the authenticity of the systems used. In the examiners' opinion, those instructions contribute to limiting over-hasty or ill-considered vote casting behaviour.
Evidence	■ https://www.evoting-info.ch/ ■ BS: https://bs.evoting.ch/ ■ GR: https://gr.evoting.ch/ ■ SG: https://sg.evoting.ch/ ■ TG: https://tg.evoting.ch/ ■ BS: https://www.bs.ch/regierungsrat/staatskanzlei/politische-rechte/wahlen-und-abstimmungen/e-voting ■ GR: https://www.gr.ch/DE/institutionen/verwaltung/staka/themen/pr-pub/evoting/Seiten/evoting-aktuell.aspx ■ SG: https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting.html ■ TG: https://rechtsdienst.tg.ch/e-voting.html/15008 ■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §3 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §4 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5 §4 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5 §4
Result	Pass
Finding	N/A

Relevance	N/A

Table 79 – Examination results: OEV paragraph 8.3

Key	8.4
Requirement	Verifiability, further security measures and the procedure in the event of anomalies are explained to voters in an accessible manner.
Observation	The *Konzept Information der Stimmberechtigten* document specifies the communication channels put in place by the cantons to detail security measures and the procedure in the event of anomalies: the cantons' website, the information platform dedicated to e-voting, the e-voting landing page itself, as well as the voting material. The multiplicity of the available channels allows the examiners to confirm the accessible nature of the information.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §3 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §4 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §4 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §4 ■ https://www.evoting-info.ch/ ■ BS: https://bs.evoting.ch/ ■ GR: https://gr.evoting.ch/ ■ SG: https://sg.evoting.ch/ ■ TG: https://tg.evoting.ch/ ■ BS: https://www.bs.ch/regierungsrat/staatskanzlei/politische-rechte/wahlen-und-abstimmungen/e-voting ■ GR: https://www.gr.ch/DE/institutionen/verwaltung/staka/themen/pr-pub/evoting/Seiten/evoting-aktuell.aspx ■ SG: https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting.html ■ TG: https://rechtsdienst.tg.ch/e-voting.html/15008
Result	Pass
Finding	N/A
Relevance	N/A

Table 80 – Examination results: OEV paragraph 8.4

Key	8.5
Requirement	Voters are told what they have to pay attention to in order to cast their vote securely.
Observation	The *Konzept Information der Stimmberechtigten* document mentions the instructions provided to the voters in order to cast their vote securely: ■ Information on e-voting security procedures (handling of the security codes), ■ Security advice with regards to technical security measures and on controlling the authenticity of the systems used.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §5 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §6 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §6 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §6

	■ https://www.evoting-info.ch/ ■ BS: https://bs.evoting.ch/ ■ GR: https://gr.evoting.ch/ ■ SG: https://sg.evoting.ch/ ■ TG: https://tg.evoting.ch/ ■ BS: https://www.bs.ch/regierungsrat/staatskanzlei/politische-rechte/wahlen-und-abstimmungen/e-voting ■ GR: https://www.gr.ch/DE/institutionen/verwaltung/staka/themen/pr-pub/evoting/Seiten/evoting-aktuell.aspx ■ SG: https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting.html ■ TG: https://rechtsdienst.tg.ch/e-voting.html/15008
Result	Pass
Finding	N/A
Relevance	N/A

Table 81 – Examination results: OEV paragraph 8.5

Key	8.6
Requirement	Voters are given instructions on how to delete their vote from all the memories on the device used for entering the vote.
Observation	The *Konzept Information der Stimmberechtigten* document mentions that instructions are provided to voters regarding the deletion of their internet browser's cache after their vote. The browser cache is the only type of memory used during the voting process.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §3.3 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §4.4 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §4.4 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §4.4 ■ https://www.evoting-info.ch/ ■ BS: https://bs.evoting.ch/ ■ GR: https://gr.evoting.ch/ ■ SG: https://sg.evoting.ch/ ■ TG: https://tg.evoting.ch/ ■ BS: https://www.bs.ch/regierungsrat/staatskanzlei/politische-rechte/wahlen-und-abstimmungen/e-voting ■ GR: https://www.gr.ch/DE/institutionen/verwaltung/staka/themen/pr-pub/evoting/Seiten/evoting-aktuell.aspx ■ SG: https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting.html ■ TG: https://rechtsdienst.tg.ch/e-voting.html/15008
Result	Pass
Finding	N/A
Relevance	N/A

Table 82 – Examination results: OEV paragraph 8.6

Key	8.7
Requirement	Voters may request support if they have questions about electronic voting.
Observation	Voters have the possibility to contact a support function, either via email or a phone number. The contact information is available on several media: cantonal website, voting material, voting portal, E-Voting landing page (and the municipalities' website in Graubünden)
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §5,6 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §6,7 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §6,7 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §6,7 ■ https://www.evoting-info.ch/ ■ BS: https://bs.evoting.ch/ ■ GR: https://gr.evoting.ch/ ■ SG: https://sg.evoting.ch/ ■ TG: https://tg.evoting.ch/ ■ BS: https://www.bs.ch/regierungsrat/staatskanzlei/politische-rechte/wahlen-und-abstimmungen/e-voting ■ GR: https://www.gr.ch/DE/institutionen/verwaltung/staka/themen/pr-pub/evoting/Seiten/evoting-aktuell.aspx ■ SG: https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting.html ■ TG: https://rechtsdienst.tg.ch/e-voting.html/15008
Result	Pass
Finding	N/A
Relevance	N/A

Table 83 – Examination results: OEV paragraph 8.7

Key	8.8
Requirement	Voters are requested to report incorrectly displayed proofs in accordance with Number 2.5 such as verification codes or other verification steps with negative results to the body responsible at cantonal level. This request is also made in the instructions sent out with the voting papers.
Observation	The *Konzept Information der Stimmberechtigten* document mentions that the cantons' website, the information platform dedicated to e-voting, as well as the voting material invite the voters to contact the cantonal authorities in case of incongruence of the security control elements during the voting process.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §3, 5 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §4,6 ■ SG,: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §4,6 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §4,6 ■ https://www.evoting-info.ch/ ■ BS: https://bs.evoting.ch/ ■ GR: https://gr.evoting.ch/ ■ SG: https://sg.evoting.ch/ ■ TG: https://tg.evoting.ch/

	■ BS: https://www.bs.ch/regierungsrat/staatskanzlei/politische-rechte/wahlen-und-abstimmungen/e-voting ■ GR: https://www.gr.ch/DE/institutionen/verwaltung/staka/themen/pr-pub/evoting/Seiten/evoting-aktuell.aspx ■ SG: https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting.html ■ TG: https://rechtsdienst.tg.ch/e-voting.html/15008
Result	Pass
Finding	N/A
Relevance	N/A

Table 84 – Examination results: OEV paragraph 8.8

Key	8.9
Requirement	Voters are requested to keep the voting papers with the security elements in fulfilment of Number 2.5 securely until they cast their final vote or until the voting process is concluded.
Observation	The *Konzept Information der Stimmberechtigten* document mentions that instructions are provided to the voters regarding the safekeeping of the voting material until the definitive casting of their vote or until the conclusion of the ballot.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §3, 5 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §4, 6 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §4, 6 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §4, 6 ■ https://www.evoting-info.ch/ ■ BS: https://bs.evoting.ch/ ■ GR: https://gr.evoting.ch/ ■ SG: https://sg.evoting.ch/ ■ TG: https://tg.evoting.ch/ ■ BS: https://www.bs.ch/regierungsrat/staatskanzlei/politische-rechte/wahlen-und-abstimmungen/e-voting ■ GR: https://www.gr.ch/DE/institutionen/verwaltung/staka/themen/pr-pub/evoting/Seiten/evoting-aktuell.aspx ■ SG: https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting.html ■ TG: https://rechtsdienst.tg.ch/e-voting.html/15008
Result	Pass
Finding	N/A
Relevance	N/A

Table 85 – Examination results: OEV paragraph 8.9

Key	8.10
Requirement	Voters are given the information required to check the authenticity of the website and the server used for voting. The informative value of a successful check must be supported by the use of cryptographic resources according to the best practices.

Observation	The e-voting landing page provides instructions for checking hash values to ensure the authenticity of the components made available to voters. Hashes are published on the e-voting landing page and on the cantonal information pages.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §3.3, 8.2 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §4.4, 9.2 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §4.3, 9.2 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §4.3, 9.2 ■ BS: https://bs.evoting.ch/ ■ GR: https://gr.evoting.ch/ ■ SG: https://sg.evoting.ch/ ■ TG: https://tg.evoting.ch/
Result	Pass
Finding	N/A
Relevance	N/A

Table 86 – Examination results: OEV paragraph 8.10

Key	8.11
Requirement	The information essential for secure voting is sent with the voting papers. Voters are told that if in doubt, they should comply with the information in the voting papers rather than the information displayed on the user device.
Observation	The *Konzept Information der Stimmberechtigten* document mentions that security advice (i.e. system compatibility for the use of the e-voting portal, check of the certificate's fingerprint, deletion of the browser's cache after the vote, check of some sensitive artefacts' hash values) is provided in the voting material. It also mentions that the voting persons are instructed to comply with the information in the voting material rather than the information displayed on the user device in case of doubt.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §5 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §4.6.1, 4.6.2, 6 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §4.5.1, 6 ■ TG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §6 ■ https://www.evoting-info.ch/ ■ BS: https://bs.evoting.ch/ ■ GR: https://gr.evoting.ch/ ■ SG: https://sg.evoting.ch/ ■ TG: https://tg.evoting.ch/ ■ BS: https://www.bs.ch/regierungsrat/staatskanzlei/politische-rechte/wahlen-und-abstimmungen/e-voting ■ GR: https://www.gr.ch/DE/institutionen/verwaltung/staka/themen/pr-pub/evoting/Seiten/evoting-aktuell.aspx ■ SG: https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting.html ■ TG: https://rechtsdienst.tg.ch/e-voting.html/15008
Result	Pass
Finding	N/A

Relevance	N/A

Table 87 – Examination results: OEV paragraph 8.11

Key	8.12
Requirement	The measures taken to preserve voting secrecy are explained to voters.
Observation	The *Konzept Information der Stimmberechtigten* document mentions that the measures to preserve voting secrecy are explained to voters on several communication channels, including the e-voting information platform.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §5 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §6 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §6 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §6 ■ https://www.evoting-info.ch/ ■ BS: https://bs.evoting.ch/ ■ GR: https://gr.evoting.ch/ ■ SG: https://sg.evoting.ch/ ■ TG: https://tg.evoting.ch/ ■ BS: https://www.bs.ch/regierungsrat/staatskanzlei/politische-rechte/wahlen-und-abstimmungen/e-voting ■ GR: https://www.gr.ch/DE/institutionen/verwaltung/staka/themen/pr-pub/evoting/Seiten/evoting-aktuell.aspx ■ SG: https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting.html ■ TG: https://rechtsdienst.tg.ch/e-voting.html/15008
Result	Pass
Finding	N/A
Relevance	N/A

Table 88 – Examination results: OEV paragraph 8.12

Key	8.13
Requirement	Known flaws and the need for action associated with them are communicated transparently.
Observation	The *Konzept Information der Stimmberechtigten* document mentions that known flaws and the need for action associated with them are communicated transparently.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §8.3 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §9.3 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §9.3 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §9.3 ■ https://www.evoting-info.ch/ ■ BS: https://bs.evoting.ch/ ■ GR: https://gr.evoting.ch/ ■ SG: https://sg.evoting.ch/ ■ TG: https://tg.evoting.ch/

	■ BS: https://www.bs.ch/regierungsrat/staatskanzlei/politische-rechte/wahlen-und-abstimmungen/e-voting ■ GR: https://www.gr.ch/DE/institutionen/verwaltung/staka/themen/pr-pub/evoting/Seiten/evoting-aktuell.aspx ■ SG: https://www.sg.ch/politik-verwaltung/abstimmungen-wahlen/e-voting.html ■ TG: https://rechtsdienst.tg.ch/e-voting.html/15008
Result	Pass
Finding	N/A
Relevance	N/A

Table 89 – Examination results: OEV paragraph 8.13

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	Members of the Electoral Board are required to undergo mandatory initial training before assuming their roles (before D2 of the electoral process). This training covers critical aspects such as: ■ Legal foundations of e-voting, ■ Role-specific responsibilities and the significance of their role in maintaining system security, ■ Key e-voting processes, including vote casting, plausibility checks, and the decryption and counting of votes, ■ Implementation of universal verifiability, including the use of the Verifier tool, ■ Emergency planning and incident management, ■ Information security instructions as per the *Richtlinie Informationssicherheit* document. Short "refresher" sessions are conducted at the start of D2 and D3 to reinforce critical knowledge. These sessions are designed to remind the present members of core concepts, particularly focusing on tasks relevant to the day. Participants receive access to crucial documents, enabling them to deepen their understanding of the training content and stay informed about necessary procedures, including checklists for D2/D3 operations. Feedback is systematically collected from participants to enhance future training sessions. Additionally, when significant technological or procedural changes occur, the training content is reviewed and updated accordingly, ensuring that personnel remain informed about the latest requirements and practices. To comply with information security guidelines, attendance lists are maintained as proof of training completion. This practice ensures traceability and accountability for the personnel involved in the e-voting processes.
Evidence	■ BS: E-Voting BS - Konzept Schulungen und interne Information – V1.1, §1.1 ■ GR: E-Voting - Konzept Schulungen und interne Information – V1.1, §2.1 ■ SG: E-Voting - Konzept Schulungen und interne Information – V1.1, §2.1 ■ TG: E-Voting-TG-Konzept-Schulungen-und-interne-Information – V1.1, §2.1 ■ BS, GR, SG, TG: E-Voting - Konzept Vollständige Verifizierbarkeit - V1.6, §6

Result	Pass
Finding	N/A
Relevance	N/A

Table 90 – Examination results: OEV paragraph 8.14

Opening and closing the electronic voting channel

Key	9
Requirement	The electronic voting channel is only available during the permitted period.
Observation	The electronic voting channel opens and closes automatically according to its configuration settings. During the configuration phase of the voting events, the persons setting up the event verify that the dates are correct. Special care is taken to verify that the dates and hours are correct in case there is a switch to or from daylight saving time between the opening and the closing of the channel
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, steps 0.10, 1.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 91 – Examination results: OEV paragraph 9

Tallying votes in the electronic ballot box

Key	11.1
Requirement	The decryption of the votes and the tallying may not begin before Polling Sunday.
Observation	The *Prozesse E-Voting* document mentions that the decryption and the tallying of the votes occur on Saturday, the day before Polling Sunday, after the closing of the electronic ballot box in the cantons of Basel-Stadt, Graubünden and St-Gallen. In the canton of Thurgau, the ballot boxes are mixed and decrypted on the voting or election day, which is Sunday. The concerned cantons have been granted a derogation to proceed before Polling Sunday.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, §3.6
Result	Pass
Finding	N/A
Relevance	N/A

Table 92 – Examination results: OEV paragraph 11.1

Key	11.2
Requirement	The canton carries out the decryption and tallying within its own infrastructure.

Observation	The decryption and tallying of the votes are performed by the members of the Admin-Board and Electoral-Board using the e-voting components managed by the cantons, in their own premises.
Evidence	■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 3.3.2 ■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §5 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §6 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §6 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §6
Result	Pass
Finding	N/A
Relevance	N/A

Table 93 – Examination results: OEV paragraph 11.2

Key	11.3
Requirement	The canton must ensure that the decryption of votes and their tallying is documented. The minutes are released by the body responsible at cantonal level.
Observation	During the decryption and tallying of the votes the Admin-Board is responsible for keeping minutes of the process. The minutes are signed by all the participants and filed physically and electronically.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 3.7, §4.4
Result	Pass
Finding	N/A
Relevance	N/A

Table 94 – Examination results: OEV paragraph 11.3

Key	11.4
Requirement	From the decryption of votes to the transmission of the result of the ballot, any access to the system or to any of its components must be made jointly by at least two persons; it must be recorded in writing and it must be possible for the examiners to check it.
Observation	The operations involving access to the e-voting system components, from the decryption of votes to the transmission of the result of the ballot, are performed by the Admin-Board in respect of the 4-eye principle. The Electoral-Board members are present and may witness the operations. The Admin-Board does not record all accesses made to the system. Instead, it attaches a copy of the operational guide that was followed to the protocol signed by all protagonists on day 3, and records all deviations from the standard procedures in the daily log. This measure satisfies the present requirement in the examiners' opinion.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, §3.6, 4.4
Result	Pass
Finding	N/A

Relevance	N/A

Table 95 – Examination results: OEV paragraph 11.4

Key	11.5
Requirement	If the result data is transmitted to a third-party system that is outside the canton's control, the data must be encrypted and signed.
Observation	The publication of the ballots' results is performed by the cantons themselves on their own information systems, hosted within the cantonal infrastructure. The results are not transmitted to any system outside the cantons' control.
Evidence	■ BS: E-Voting BS - Konzept E-Voting - V1.6, §7.3.1 ■ GR: E-Voting - Konzept E-Voting – V1.3, §8.3.1 ■ SG: E-Voting - Konzept E-Voting – V1.6, §8.3.1 ■ TG: E-Voting-TG-Konzept E-Voting – V1.6, §8.3.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 96 – Examination results: OEV paragraph 11.5

Key	11.6
Requirement	The system allows the polling card to be used to determine whether someone has cast an electronic vote.
Observation	Each polling card includes a barcode, which can be scanned using the Post's Voting Card Manager (VCM) tool to check whether an electronic vote has already been cast.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step A9
Result	Pass
Finding	N/A
Relevance	N/A

Table 97 – Examination results: OEV paragraph 11.6

Key	11.7
Requirement	Auditors must be present during decryption and tallying. The canton may permit additional remote auditing work.
Observation	The *Konzept Vollständige Verifizierbarkeit* document specifies that the auditors must be present during decryption and tallying.
Evidence	BS, GR, SG, TG: E-Voting - Konzept Vollständige Verifizierbarkeit - V1.6, §3.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 98 – Examination results: OEV paragraph 11.7

Key	11.8
Requirement	If components used to tally votes are not trustworthy in accordance with Number 2.4, the same requirements apply to these components as to set-up components under Number 3.
Observation	The votes are tallied on the control component hosted at the cantons' (a.k.a. the *tally computer*). The requirements applying to set-up components under Number 3 include Numbers 3.1, 3.2, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.14, 3.17, 3.19, 3.20. The measures to comply with these requirements are uniformly applied to all e-voting computers, including the tally computer.
Evidence	Audit results for Numbers 3.1, 3.2, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.14, 3.17, 3.19, 3.20.
Result	Pass
Finding	N/A
Relevance	N/A

Table 99 – Examination results: OEV paragraph 11.8

Key	11.9
Requirement	The auditors exercise their responsibility in accordance with cantonal law when examining the proofs in accordance with Number 2.6.
Observation	The ordinance of the canton of Basel-Stadt related to e-voting tests defines the following tasks for an election committee: Encryption and provision of the electronic ballot box, delivery of the control votes, decryption of the ballot box and verification of the control votes on the Sunday of voting. The ordinance on political rights in the canton of Graubünden defines the tasks, duties and competences of the E-Voting Election and Voting Commission. In particular, its members, as auditors, check the evidence generated in connection with universal verifiability. The cantonal law of the canton of St. Gallen on elections and voting requires the government to elect a voting office which supervises the determination of the results, releases the results for official publication and supervises the decoding of the electronic ballot box. The ordinance to the Act on voting and election rights of the canton of Thurgau states that the voting office monitors the process, the decoding and the evaluation of the votes cast electronically. Thus, when examining the proofs in accordance with Number 2.6, the auditors exercise their responsibility in accordance with cantonal law.
Evidence	■ BS, GR, SG, TG: E-Voting - Konzept Vollständige Verifizierbarkeit - V1.6, §3.1 ■ BS: Verordnung über den Testbetrieb für die elektronische Stimmabgabe 132.150 ■ GR: Verordnung über die politischen Rechte im Kanton Graubünden (VPR; BR150.200) ■ SG: Gesetz über Wahlen und Abstimmungen St. Gallen Art.12 ■ TG: Verordnung des Regierungsrates zum Gesetz über das Stimm- und Wahlrecht (StWV)

Result	Pass
Finding	N/A
Relevance	N/A

Table 100 – Examination results: OEV paragraph 11.9

Key	11.10
Requirement	The body responsible at cantonal level submits all relevant indicators of the correctness of the result to the auditors. This includes, in addition to the proofs in accordance with Number 2.6, in particular the number and nature of anomalies reported to the canton by voters.
Observation	The correctness of the results is controlled using the verification tool (a.k.a., the *Verifier*) of the Post, which provides the proofs in accordance with Number 2.6. The *Konzept Vollständige Verifizierbarkeit* mentions that the auditors receive the number and type of anomalies reported to the cantons by persons entitled to vote, as well as reports and indications from the post office or third parties.
Evidence	■ BS, GR, SG, TG: E-Voting - Konzept Vollständige Verifizierbarkeit - V1.6, §3.1.2 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 3.4
Result	Pass
Finding	N/A
Relevance	N/A

Table 101 – Examination results: OEV paragraph 11.10

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	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 anomalies analyses.
Evidence	■ BS, GR, SG, TG: E-Voting - Konzept Vollständige Verifizierbarkeit - V1.6, §5 ■ BS, GR, SG, TG: E-Voting - Notfallplan - V1.6
Result	Pass
Finding	N/A
Relevance	N/A

Table 102 – Examination results: OEV paragraph 11.11

Key	11.12
Requirement	Statistical methods must be used to check the plausibility of the result, provided they are available and there is sufficient data.
Observation	To check the plausibility of the results, the cantons use the following means:

	■ The members of the voting office set a control ballot box and cast test votes during the initialisation phase of a ballot. They record their choices and store them in a sealed envelope. During the counting of votes, the results of the control box are compared to the votes cast by the voting office members to verify that those votes were processed and counted correctly, ■ They reconcile the number of votes counted electronically with the Post's statistical reports, ■ They compare the results of the electronic ballots with the final results in order to identify significant discrepancies between the voting channels.
Evidence	■ BS: E-Voting - Konzept E-Voting – V1.6, §5.8 ■ GR: E-Voting - Konzept E-Voting – V1.3, §6.8 ■ SG: E-Voting - Konzept E-Voting – V1.6, §6.8 ■ TG: E-Voting-TG-Konzept E-Voting – V1.6, §6.10 ■ BS, GR, SG, TG: E-Voting - Konzept Vollständige Verifizierbarkeit - V1.6, §2 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, steps 2.9, 3.4.4, 3.4.6, §4.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 103 – Examination results: OEV paragraph 11.12

Confidential data

Key	12.1
Requirement	It is guaranteed that neither employees nor externals hold data that allow a connection to be made between the identity of persons voting and the votes they have cast.
Observation	Voting secrecy is one of the properties that must be provided by electronic voting (as per federal law requirement). The e-voting system is designed in a way that allows to determine whether a voting card has been used but without knowing the identity of the voter nor how he/she voted.
Evidence	■ BS: E-Voting BS - Konzept E-Voting - V1.6, §5.6 ■ GR: E-Voting - Konzept E-Voting – V1.3, §6.8 ■ SG: E-Voting - Konzept E-Voting – V1.6, §6.6 ■ TG: E-Voting-TG-Konzept E-Voting – V1.6, §6.8
Result	Pass
Finding	N/A
Relevance	N/A

Table 104 – Examination results: OEV paragraph 12.1

Key	12.2
Requirement	It is guaranteed that neither employees nor externals hold data before the decryption of the votes that allow the premature determination of partial results.
Observation	The cryptographic protocol of the e-voting system guarantees the secrecy of votes: The cast votes are subject to client-side encryption and are only stored in an encrypted way. The determination of results or partial results requires the decryption of the votes.

	From the organisational point of view, the *Konzept Vollständige Verifizierbarkeit* document makes the auditors accountable for the preservation of the voting secrecy.
Evidence	BS, GR, SG, TG: E-Voting - Konzept Vollständige Verifizierbarkeit - V1.6, §3.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 105 – Examination results: OEV paragraph 12.2

Key	12.3
Requirement	The canton may not pass on to private companies its part of the key for decrypting the votes which it has on the control component that it operates in accordance with Number 3.1.
Observation	The *Prozesse E-Voting* document shows that the ballot decryption process is performed solely by the members of the Admin-Board and Electoral-Board. No e-voting process involves the communication of the decryption key to any third-party.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8
Result	Pass
Finding	N/A
Relevance	N/A

Table 106 – Examination results: OEV paragraph 12.3

Key	12.4
Requirement	The canton must treat the results of the ballot as confidential between the time the votes are decrypted and the time of publication.
Observation	The *Prozesse E-Voting* document mentions that, once decrypted, the results of a ballot must be treated as confidential until they are published. According to the *Konzept Vollständige Verifizierbarkeit* document, the auditors are subject to a confidentiality duty regarding those results until publication.
Evidence	■ BS, GR, SG, TG: E-Voting - Konzept Vollständige Verifizierbarkeit - V1.6, §3.2 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 3.4.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 107 – Examination results: OEV paragraph 12.4

Key	12.5
Requirement	The canton must ensure that data that indicate whether a voter has voted electronically are treated as confidential.

Observation	Voters may contact the cantons to verify that their electronic vote has been cast effectively. In such case, the cantons are able to determine whether a given voting card number has been used to cast a vote. The communes need also this information when duplicates of the voting cards need to be issued (when a voter claims that the original voting card has been lost, and to ensure that voters do not vote twice via different channels). The risk analysis performed by the cantons mentions that the register of voting cards is to be treated as confidential (its access should be restricted to the State Chancellery and the communes). A specific mention regarding the confidential nature of this data can be found in the document *Anleitung für die Gemeinden.*
Evidence	■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 4.4 ■ BS, GR, SG, TG: E-Voting - P18 - Register der Stimmrechtsausweise (Profil) ■ BS: E-Voting - Anleitung für die Gemeinden – V1.4, §7 ■ GR: E-Voting - Anleitung für die Gemeinden – V12, §7 ■ SG: E-Voting SG - Anleitung für die Gemeinden – V1.6, §6 ■ TG: E-Voting – TG – Anleitung für die Gemeinden – V0.9, §7
Result	Pass
Finding	N/A
Relevance	N/A

Table 108 – Examination results: OEV paragraph 12.5

Key	12.6
Requirement	The canton must treat the individual votes as confidential after they have been tallied.
Observation	The *Prozesse E-Voting* document mentions that, once the votes have been tallied, they must be kept confidential until their official publication.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 3.4.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 109 – Examination results: OEV paragraph 12.6

Key	12.7
Requirement	The canton must ensure that vote and election results in small constituencies are treated as confidential.
Observation	In a ballot, the voting secrecy principle might be compromised if, for instance, all voters vote the same way. Such situation is more likely to occur in smaller municipalities. In such case, the cantons choose to aggregate the results of different municipalities.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §7.2 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §8.2 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §8.2 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §8.2

Result	Pass
Finding	N/A
Relevance	N/A

Table 110 – Examination results: OEV paragraph 12.7

Key	12.8
Requirement	Following validation and in accordance with a predetermined and documented process, all data created as part of the electronic ballot that relate to the individual votes received and that are classified as confidential must be destroyed.
Observation	For the evaluation of this criterion, the examiners consider that the data referred to as "all data created as part of the electronic ballot that relate to the individual votes received" correspond to the information asset *electronic votes* defined by the cantons in their risk assessment. Electronic votes are assigned the secret confidentiality classification. According to the *Inventar der Informationsressourcen* document, the technical containers for the electronic votes include: USB memory sticks, the online computer, the tally computer, the infrastructure of the Post. During the *Preparation of the ballot* phase, all laptops are reinstalled and the USB memory sticks that were used in a previous ballot are erased using the *sDelete* software and reformatted, except the ones used for data backup if the legal retention period has not expired.
Evidence	■ Risikobeurteilung - Inventar der Informationsressourcen ■ BS, GR: SG. TG: Prozesse E-Voting V1.8, step 0.3.3, §4.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 111 – Examination results: OEV paragraph 12.8

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	The threats listed in the Numbers 13.3-13.40 are all considered in the cantons' risk assessment of the e-voting system. The list is supplemented by additional threats elicited through the risk assessment methodology.
Evidence	Profile Informationsressourcen
Result	Pass
Finding	N/A

Relevance	The requirement includes a translation error: “this must be added to” (German version: “,die zu ergänzen ist”)

Table 112 – Examination results: OEV paragraph 13.1

Key Requirement	13.2		
	The following are considered to be potential threats: inadvertent or intended electronic or physical threats from internal or external actors; threats resulting from a malfunction of the system or system-supporting elements		
		Description	**Security objective concerned (in accordance with Art. 4 para. 3)**
	13.3	Malware changes the vote on the user device.	Accuracy of the result
	13.4	An external attacker redirects the vote using domain name server spoofing (DNS spoofing)6.	Accuracy of the result
	13.5	An external attacker changes vote using the man-in-the-middle (MITM) technique7.	Accuracy of the result
	13.6	An external attacker sends a maliciously altered ballot paper using MITM.	Accuracy of the result
	13.7	An internal attacker manipulates the software, causing it not to store the votes.	Accuracy of the result
	13.8	An internal attacker changes the votes.	Accuracy of the result
	13.9	An internal attacker inserts votes.	Accuracy of the result
	13.10	A hostile organisation infiltrates the system with the aim of falsifying the result.	Accuracy of the result
	13.11	An internal attacker copies voting papers and uses them.	Accuracy of the result
	13.12	An external attacker uses social engineering techniques to distract the person voting from following the security measures (individual verifiability).	Accuracy of the result

[6] Also known as DNS poisoning. This is an attack which successfully falsifies the correlation between a host name and the related IP address.

[7] The attacker in a man-in-the-middle attack. This is a type of attack used in computer networks. The attacker is positioned either physically or logically between the two communication partners and via its system has full control of the data traffic between two or more network participants and can view or even manipulate any information it wants.

[redacted]	13.13	An external attacker infiltrates the canton's infrastructure electronically, physically or by means of social engineering and extracts security-relevant data while the parameters of the ballot are being set.	Accuracy of the result
	13.14	An external attacker infiltrates the printing office's infrastructure electronically, physically or by means of social engineering and extracts the codes of the polling cards.	Accuracy of the result
	13.15	An external attacker infiltrates the postal service's infrastructure electronically, physically or by means of social engineering and steals polling cards.	Accuracy of the result
	13.16	An error occurs in the individual verifiability.	Accuracy of the result
	13.17	An error occurs in the universal verifiability.	Accuracy of the result
	13.18	An error occurs in an auditor's technical aid.	Accuracy of the result
	13.19	A backdoor8 is introduced into the system via a software dependency and is exploited by an external attacker to access the system.	Accuracy of the result, preservation of voting secrecy and exclusion of premature results, accessibility and operability of the voting system, protection of information intended for voters from manipulation, prevention of improper use of evidence of voting behaviour
	13.20	Malware on the user device sends the vote to a hostile organisation.	Preservation of voting secrecy and exclusion of premature results
	13.21	The vote is redirected using DNS spoofing.	Preservation of voting secrecy and exclusion of premature results
	13.22	An external attacker reads a vote using MITM.	Preservation of voting secrecy and exclusion of premature results
	13.23	An internal attacker uses the key and decrypts non-anonymous votes.	Preservation of voting secrecy and exclusion of premature results
	13.24	While checking the accuracy of the processing and tallying, voting secrecy is breached.	Preservation of voting secrecy and exclusion of premature results

[8] A backdoor is a portion of software that allows access to the computer or an otherwise protected function of a computer program by bypassing normal access protections.

[redacted]	13.25	An internal attacker reads the votes at an early stage without having to decrypt the votes.	Preservation of voting secrecy and exclusion of premature results
	13.26	A hostile organisation infiltrates the system with the aim of breaching voting secrecy or obtaining premature results.	Preservation of voting secrecy and exclusion of premature results
	13.27	An error in the encryption process renders it inoperable or reduces its effectiveness.	Preservation of voting secrecy and exclusion of premature results
	13.28	Malware on the user device makes voting impossible.	Accessibility and operability of the voting system
	13.29	A hostile organisation carries out a denial-of-service (DOS)9 attack.	Accessibility and operability of the voting system
	13.30	An internal attacker carries out an incorrect configuration; it does not get to the tallying.	Accessibility and operability of the voting system
	13.31	An internal attacker falsifies the cryptographic proofs of universal verifiability.	Accessibility and operability of the voting system
	13.32	A technical error in the system causes the system to be unavailable at the time of the count.	Accessibility and operability of the voting system
	13.33	One of the auditors' technical aids does not work at the time of tallying.	Accessibility and operability of the voting system
	13.34	A hostile organisation infiltrates the system with the aim of disrupting operations, manipulating voter information or stealing proofs of the voting behaviour of the persons voting.	Accessibility and operability of the voting system, protection of information intended for voters from manipulation, prevention of improper use of evidence of voting behaviour
	13.35	An internal attacker steals voters' address data.	Protection of personal information relating to voters
	13.36	Malware influences voters' opinions.	Protection of information intended for voters from manipulation
	13.37	An internal attacker manipulates the information website or voting portal and thereby deceives voters.	Protection of information intended for voters from manipulation

[9] In digital data processing, this is the non-availability of a service that should be available.

	13.38	An internal attacker tells voters whether and how they have to vote. After decryption, he finds evidence in the infrastructure that the voters have followed the instructions.	Prevention of improper use of evidence of voting behaviour
	13.39	An external attacker tells voters whether and how they have to vote and demands evidence that they have followed the instructions.	Prevention of improper use of evidence of voting behaviour
Observation	The risk assessment performed by the cantons on the e-voting system bases upon the OCTAVE Allegro methodology, which considers the following threat agents: ■ Human actors using technical means, ■ Human actors using physical means, ■ Technical problems. Human actors considered include internal (e.g. employees) and external (e.g. suppliers, Internet hackers) actors.		
Evidence	■ BS, GR, SG, TG: E-Voting - Richtlinie Risikomanagement V1.2, §5.1 ■ BS, GR, SG, TG: E-Voting - Risikoportfolio		
Result	Pass		
Finding	N/A		
Relevance	N/A		

Table 113 – Examination results: OEV paragraph 13.2

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

Key	14.1
Requirement	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. 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.
Observation	Monitoring activities are managed by the provider of the e-voting system (i.e. the Swiss Post). The Prozesse *E-Voting* document mentions that, during the voting period, the cantons receive a daily report from the Post detailing the results of the monitoring activities. Events reported are documented in an event book. The cantons have drafted a high-level emergency plan in case errors are detected by the Verifier or incidents detected through monitoring activities. The plan includes a definition of the roles and responsibilities as well as a notification to the state Chancellery in such case.

Evidence	■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, steps A6, A8, 3.4.2 ■ BS, GR, SG, TG: E-Voting - Notfallplan - V1.6, §3.1, 3.2.5, 3.2.6
Result	Pass
Finding	N/A
Relevance	N/A

Table 114 – Examination results: OEV paragraph 14.1

Key	14.2
Requirement	Records are created on the infrastructure whose recording, transmission and storage are resistant to manipulation (system logs). The records are consistent with each other and allow the relevant events to be traced when investigating suspected manipulation or errors. They serve as evidence of the complete, unfalsified and exclusive tallying of votes cast in conformity with the system, of preservation of voting secrecy and of the exclusion of premature partial results. The content of the records covers at least the following events: ■ start and end of the audit, identification and authentication processes; ■ start, restart and end of the voting or election phase; ■ start of the tallying with the determination of the results; ■ conduct and results of any self-tests; ■ malfunctions identified in elements of the IT infrastructure that affect the ability to operate. The date and time of each event, the type of event, the possible originator and the result in terms of failure or success are documented. The system logs are made available to the body responsible at cantonal level in such a way that it can interpret the information.
Observation	The different elements of the e-voting system generate system logs. The processes for the generation and protection of those records is the Post's responsibility. The system logs are made available to the cantons on a daily basis under the form of dashboards and statistics issued by the Post's security information and event management (SIEM) system. The *Notfallplan* document details the reaction process to incidents detected through monitoring activities. It mentions that relevant system logs are provided to the cantons on demand in such circumstances.
Evidence	■ BS, GR, SG, TG: E-Voting - Notfallplan - V1.4, §3.2.5 ■ Sample Splunk report
Result	Pass
Finding	N/A
Relevance	N/A

Table 115 – Examination results: OEV paragraph 14.2

Key	14.3

Requirement	The monitoring and recording of system logs are subject to a continuous improvement process. The improvement process involves an open dialogue between those involved and a regular and objective assessment of the effectiveness of the instruments and processes used. The results of these evaluations will be taken into account.
Observation	The *Prozesse E-Voting* document mentions that the Admin-Board participates to a *lessons learned* session after each ballot in order to improve the e-voting processes. When faults or anomalies are reported during a ballot, investigations are conducted. The Admin-Board also analyses whether all required information was made available and takes appropriate measures if needed.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, steps 4.3, 4.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 116 – Examination results: OEV paragraph 14.3

Key	14.4
Requirement	The monitoring and recording of system logs in no way detracts from the effectiveness of the measures taken to preserve voting secrecy.
Observation	The monitoring and recording of system logs are performed by the e-voting system provider, i.e. the Swiss Post. The contract between the cantons and Swiss Post mandates that the system delivered by the Post conforms to the ordinance on electronic voting and thus creates appropriate logs.
Evidence	BS, GR, SG, TG: Contract between Swiss Post and the cantons, Appendix A, §1.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 117 – Examination results: OEV paragraph 14.4

Key	14.7
Requirement	It is possible to cast control votes using authentication credentials that are not assigned to any voter. The content of these control votes is recorded. The tallying of the control votes is compared with the records. It must be ensured that the control votes are dealt with in as similar a way possible as votes cast in conformity with the system, while at the same time ensuring that they are not counted.
Observation	The *Prozesse E-Voting* document describes how control votes are generated, imported into the system, submitted (one vote per member of the voting office) and checked (the voting office members verify that the vote they have cast are identical to the votes tallied) as part of an electronic ballot. The voting procedure is the same for control votes as for regular votes. Control votes are cast into a dedicated ballot box to ensure that they are not counted.

Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, steps 0.9, 1.1, 2.9, SRA-3, 3.4.4, 3.4.6
Result	Pass
Finding	N/A
Relevance	N/A

Table 118 – Examination results: OEV paragraph 14.7

Key	14.8
Requirement	Infrastructure availability must be checked and recorded at selected intervals.
Observation	During the voting period, the cantons regularly cast a vote with specific test polling cards, which allows verifying that the infrastructure is available.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step A4
Result	Pass
Finding	N/A
Relevance	N/A

Table 119 – Examination results: OEV paragraph 14.8

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	During the preparation phase of a ballot, the Admin-Board reviews the weaknesses affecting the components of the e-voting system under their control (i.e. the laptops) that have been published and decide whether those components must be updated. Updates are not performed directly on the computers. Instead, a new image including the latest updates available is created and installed in offline mode. This operation occurs 11 to 12 weeks before a ballot and is subject to formal management authorisation. After this period, if a vulnerability is disclosed, the provider of the e-voting system (i.e. the Swiss Post) alerts the cantons and a risk-based decision is taken.
Evidence	■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 0.3.2 ■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §4 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §5 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §5 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §5 ■ BS, GR, SG, TG: E-Voting - Basic installation and hardening - V1.7
Result	Pass
Finding	N/A
Relevance	N/A

Table 120 – Examination results: OEV paragraph 14.9

Key	14.10
Requirement	The measures for monitoring and keeping records of system usage, the activities of administrators and of malfunction records must be described in detail, implemented, monitored and reviewed.
Observation	Monitoring activities related to the e-voting system are performed by the Post and provided to the cantons under the form of reports. On the cantons' side, several steps of the e-voting process performed by the Admin-Board members are logged, including all accesses to and usage of trustworthy components. During the whole lifecycle of a ballot, relevant events are logged in a logbook (errors reported by the Post regarding the registration of the votes, malfunctions at the infrastructure level, changes in access rights, anomalies reported through support requests). Those elements are reviewed after the closing of the ballot and lessons learned integrated into the processes when necessary.
Evidence	■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step A8, step 3.4.1, §3.7, step §4.4 ■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §2.5 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §3.5 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §3.5 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §3.5 ■ Ereignisbuch canton Thurgau – February 2025 ballot ■ Beispiel_täglicher_Splunkbericht_während_Urnenöffnungszeit_TG-2025-02-04.pdf
Result	Pass
Finding	N/A
Relevance	N/A

Table 121 – Examination results: OEV paragraph 14.10

Use of cryptographic measures and key management

Key	15.1
Requirement	Electronic certificates must be managed according to the best practices.
Observation	Electronic certificates play a critical role in multiple e-voting processes, such as: ■ The secure transmission of voter credentials, ■ The integrity of election data exchanges, ■ The encryption and signing of votes, ■ The authentication and the verification of the integrity of trusted system components. The *Richtlinie Informationssicherheit* document indicates that electronic certificates used by the canton in the context of e-voting are managed "according to best practices". This document, as well as the Post's operational guide (*Benutzeranleitung*) describe the practices applied to the management of electronic certificates: ■ Public keys are exchanged and verified following Direct Trust principles, where fingerprint verification is conducted separately through either a physical meeting or a secure online channel,

	■ Private keys are stored only on offline computers or encrypted storage devices, and access is restricted via the four-eyes principle, ■ Cryptographic algorithms used are compliant with the eCH-0014 standard, ensuring that the key lengths and algorithms used correspond to the current standards, ■ Passwords used to protect private keys are generated using sufficient entropy to resist brute-force attacks. The Post's operational guide outlines the detailed steps for the Direct Trust process.
Evidence	■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.3 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.3 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.3 ■ TG: E-Voting-TG-Richtlinie Informationssicherheit – V1.6 §4.3 ■ Benutzeranleitung (OG Post) Release 1.4 v.11 §10.2
Result	Potential improvement
Finding	The cantons do not provide any detail regarding the "best practices" in place to manage certificates used on the informational cantonal websites dedicated to e-voting.
Relevance	N/A

Table 122 – Examination results: OEV paragraph 15.1

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	The *Richtlinie Informationssicherheit* document mentions that the rules for the management of cryptographic measures are defined by the Post (generation, usage and protection of cryptographic keys). It details the best practice cryptographic measures applied to enforce the integrity of the ballots' results and the confidentiality of the authorities' identification and authentication data (see audit observation for §15.1 here above).
Evidence	■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.3 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.3 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.3 ■ TG: E-Voting-TG-Richtlinie Informationssicherheit – V1.6, §4.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 123 – Examination results: OEV paragraph 15.2

Key	15.3
Requirement	To ensure that critical data are kept secret, effective cryptographic measures are used in the infrastructure that correspond to the state of the art. Such data is always stored encrypted on data carriers.

Observation	From the canton's perspective, the infrastructure components storing the e-voting critical data include laptops and USB memory sticks serving as data carriers. The laptops' hard disk drives are encrypted using the OS' native solution (BitLocker). The data stored on the USB sticks is encrypted either by the e-voting software, by using a third-party software provided by the Post, or by using hardware-encrypted USB drives.
Evidence	■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §3.2 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §4.2 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §4.2 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §4.2 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, §3.4, step SRA-1
Result	Pass
Finding	N/A
Relevance	N/A

Table 124 – Examination results: OEV paragraph 15.3

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	The document *Richtlinie Informationssicherheit* includes a paragraph on the use of cryptography, stating that cryptographic measures must conform to the eCH-0014 standard. The operational guide specifies the algorithms used for the signature and encryption of data transmitted to the print offices (RSASSA-PSS algorithm with SHA-256 hash and 3072-bit key length), which are compliant with the requirements. According to tables 15, 16 and 17 of the S*ystem specification* document, there are 27 cases where signatures are used by the cryptographic protocol supporting the e-voting system. The certificates used for these signatures are generated by each component according to the direct trust model introduced with version 1.3 of the system. The signature seems to meet the requirements of advanced signatures according to ESigA. However, the certificates do not "originate from a recognised supplier of certificate services under the ESigA" as required. Additionally, a separate certificate is used by the VCPS tool to sign the PDF version of the voting cards prior to transmitting them to the print office (in Basel-Stadt, Graubünden and Thurgau). This certificate is also generated locally on an offline computer and exchanged securely with the print office. Again, the signature seems to meet the requirements of advanced signatures but the certificate does not originate from a recognised supplier of certificate services under the ESigA.
Evidence	■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.3 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.3 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.3 ■ TG: E-Voting-TG-Richtlinie Informationssicherheit – V1.6, §4.3 ■ Benutzeranleitung (OG Post) Release 1.4 v.11 ■ Swiss Post Voting System – System specification – V1.4.1.1 §7

Result	Partially fail
Finding	Although their security level may be equivalent, the certificates used in the direct trust model do not originate from a recognised supplier of certificate services under the ESigA.
Relevance	The need to use certificates that have been issued by a recognised supplier of certificate services under the ESigA does not seem to be justified from an information security standpoint for some of the use cases of the cantons. When installed on an offline device, it is not possible to check the Certificate Revocation List (CRL) of the corresponding issuing certificate authority, which runs contrary to good practices in terms of qualified certificate management. Moreover, suppliers of ESigA certificates do not seem to supply signing certificates for machines.

Table 125 – Examination results: OEV paragraph 15.4

Secure electronic and physical exchange of information

Key	16.1
Requirement	All infrastructure components must be operated in a separate network zone. This network zone must be protected in relation to other networks by an appropriate routing control.
Observation	The only component that connects to a network is the online computer, which uploads the lists of voters to the e-voting portal operated by the Post. According to the *Hardware und Infrastruktur* and *Richtlinie Informationssicherheit* documents, the cantons use a dedicated network segment for the online computer.
Evidence	■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §7 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §8 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §8 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §8 ■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.11 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.11 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.11 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4.11
Result	Pass
Finding	N/A
Relevance	N/A

Table 126 – Examination results: OEV paragraph 16.1

Key	16.2
Requirement	As a principle, electronic voting should be clearly separated from all other applications.
Observation	On the cantons' side, the electronic voting application components run on dedicated hardware.
Evidence	■ BS: E-Voting BS - Hardware und Infrastruktur – V1.5, §3 ■ GR: E-Voting - Hardware und Infrastruktur – V1.1, §4 ■ SG: E-Voting - Hardware und Infrastruktur – V1.4, §4 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.4, §4

Result	Pass
Finding	N/A
Relevance	N/A

Table 127 – 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	The *Konzept E-Voting* document lists the roles responsible for all operational steps executed during a ballot. The cantons maintain a list of all individuals involved in the operation of a given electoral event, and their role.
Evidence	■ BS: E-Voting BS - Konzept E-Voting - V1.6, §3 ■ GR: E-Voting - Konzept E-Voting – V1.3, §4 ■ SG: E-Voting - Konzept E-Voting – V1.6, §4 ■ TG: E-Voting-TG-Konzept E-Voting – V1.6, §4 ■ BS, GR, SG, TG: E-Voting - Personalliste (Vorlage)
Result	Pass
Finding	N/A
Relevance	N/A

Table 128 – 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	The *Hardware und Infrastruktur* document provides details regarding the installation of the e-voting components under the cantons' responsibility (hardware, software, access rights). During the preparation phase of a ballot, the Admin-Board decides whether the e-voting laptops must be updated and provides formal authorisation where applicable. The *Richtlinie Informationssicherheit* document specifies that changes to the infrastructure is subject to a change management process, and therefore are subject to formal approval.
Evidence	■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §4 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §5 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §5 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §5 ■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.10 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.10 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.10 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4.10 ■ BS, GR, SG, TG: Prozesse E-Voting V1.8, step 0.3.2

Result	Pass
Finding	N/A
Relevance	N/A

Table 129 – Examination results: OEV paragraph 18.2

Key	18.3
Requirement	The risks in connection with third parties (contractors such as suppliers and service providers) must be identified and if necessary reduced by means of suitable contractual agreements. Compliance with the agreements must be appropriately monitored and reviewed throughout their term.
Observation	The cantons' risk portfolio includes entries that concern third parties involved in the e-voting (mainly the Swiss Post and the print offices) specifically, as well as other risks where the threat actor may be a third party. The *Richtlinie Informationssicherheit* document mentions that the cantons have concluded written contracts with all suppliers involved in the e-voting operations. The third parties are required to implement the necessary security measures to reduce the risks to an acceptable level. The cantons reserve the right to require a status regarding the implementation of applicable security measures and to audit the concerned third-parties.
Evidence	■ E-Voting – Riskportfolio ■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.5, §3.9 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.1, §4.9 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.5, §4.9 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.5, §4.9 ■ BS: E-Voting BS - Prozessbeschreibung für die Produktion von E-voting-Stimmrechtsausweisen_Baumer - V2.0 ■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1_sig ■ TG: E-voting-TG- Prozessbeschreibung für die Produktion ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 ■ von E-Voting-Stimmrechtsausweisen-V2.0
Result	Pass
Finding	N/A
Relevance	N/A

Table 130 – Examination results: OEV paragraph 18.4

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	The cantons have identified their information assets as part of their risk assessment. The risk assessment basing upon the Octave Allegro methodology, the assets inventory is split into two categories: information assets (i.e., the various types of information processed within the e-voting system) and containers (i.e., the processing facilities for the information assets). Processes are not inventoried. A list of the human resources involved in the e-voting processes is drawn up for each ballot.
Evidence	■ BS, GR, SG, TG: E-Voting - Inventar der Informationsressourcen ■ BS, GR, SG, TG: E-Voting - Personalliste E-Voting (Vorlage) ■ BS, GR, SG, TG: E-Voting – Prozesse E-Voting – V1.8, step 0.2
Result	Pass
Finding	The cantons do not maintain an inventory of the e-voting processes.
Relevance	Given the risk assessment methodology adopted by the canton, the examiners estimate that an inventory of the e-voting processes is not necessary.

Table 131 – Examination results: OEV paragraph 19.1

Key	19.2
Requirement	The acceptable use of intangible and tangible resources must be defined.
Observation	The cantons maintain an inventory of the information assets (i.e., types of data), as well as their containers (i.e., the information processing facilities) that form the e-voting system. The *Richtlinie Informationssicherheit* document mentions that the e-voting information processing facilities under the cantons' responsibility (i.e., laptops, data carriers) must be managed following the procedures depicted in the *Prozesse E-Voting* and *Hardware und Infrastruktur* documents. Moreover, the document mandates: ■ Secure handling, storage and disposal of physical assets, ■ Proper classification and protection of sensitive data, ■ Strict access control to resources and separation of duties, ■ Secure management of cryptographic resources.
Evidence	■ BS, GR, SG, TG: E-Voting - Inventar der Informationsressourcen ■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4 ■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2

	■ SG: E-Voting - Hardware und Infrastruktur – V1.5 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 132 – Examination results: OEV paragraph 19.2

Key	19.3
Requirement	Classification guidelines for information must be issued and communicated.
Observation	The *Inventar der Informationsressourcen* document details the confidentiality level of each e-voting asset. The *Richtlinie Informationssicheirheit* document defines the classification levels. The *Prozesse E-Voting* document describes how assets are handled during each step of an electronic ballot.
Evidence	■ BS, GR, SG, TG: E-Voting - Inventar der Informationsressourcen ■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.2 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.2 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.2 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4.2 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8
Result	Pass
Finding	N/A
Relevance	N/A

Table 133 – Examination results: OEV paragraph 19.3

Key	19.4
Requirement	Procedures must be devised for the labelling and handling of information.
Observation	The *Richtlinie Informationssicherheit* document mandates the use of a confidentiality grade (*nicht klassifiziert*, *vertraulich, geheim* for the cantons of Graubünden, St. Gallen and Thurgau, *geheim*, *vertraulich* for the canton of Basel-Stadt) for information assets. The *Dokumentmanagement* document mandates the use of a confidentiality label in the e-voting documents (*öffentlich*, *intern*, *vertraulich*, *geheim* for the canton of Basel-Stadt, *keine*, *intern*, *vertraulich* for the cantons of Graubünden, St. Gallen and Thurgau) The *Prozesse E-Voting* document describes how assets are handled during each step of the e-voting process.
Evidence	■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.2 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.2 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.2 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4.2 ■ BS: E-Voting BS – Dokumentenmanagement – V1.1, §1.5 ■ GR: E-Voting – Dokumentmanagement – V1.0, §2.5 ■ SG: E-Voting – Dokumentmanagement – V1.1, §2.5 ■ TG: E-Voting – TG - Dokumentenmanagement – V1.0, §2.5 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8

Result	Pass
Finding	N/A
Relevance	N/A

Table 134 – Examination results: OEV paragraph 19.4

Trustworthiness of human resources

Key	20.1
Requirement	Suitable policies and procedures must be devised and promulgated in order to guarantee the trustworthiness of human resources before, during and after termination of employment or in the case of a change of activity.
Observation	The *Richtlinie Informationssicherheit* document includes a chapter related to personnel security. It mentions the existence of security rules that apply to the personnel involved in the e-voting processes. It also points to cantonal regulations that define the obligations of state employees (e.g. loyalty duty, official secrecy, etc.).
Evidence	■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.1 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, § 4.1 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.1 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4.1 ■ BS: Weisung Schutzmassnahmen Informationssicherheit ■ BS: Weisung für die Benutzung von Informatikmitteln in der Verwaltung des Kantons Basel-Stadt ■ BS: Personalgesetz (SG 162.100) ■ GR: Gesetz über das Arbeitsverhältnis der Mitarbeitenden des Kantons Graubünden (PG, BR 170.400) ■ SG: Verordnung über die Informatiksicherheit vom 24.02.2004 (sGS 142.21) ■ SG: Personalgesetz vom 25.01.2011 (PersG, sGS 143.1) ■ TG: Verordnung über die Rechtsstellung des Staatspersonals (RSV; RB 177.112)
Result	Pass
Finding	N/A
Relevance	N/A

Table 135 – Examination results: OEV paragraph 20.1

Key	20.2
Requirement	Heads of human resources must accept full responsibility for guaranteeing the trustworthiness of human resources.
Observation	The *Richtlinie Informationssicherheit* document details the responsibilities for the implementation of the security measures applying to the e-voting processes. The head of the state chancellery is responsible for the trustworthiness of human resources working with e-voting.
Evidence	■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §2.2.1, 3.1 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §3.2.1, 4.1 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §3.2.1, 4.1

	■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §3.2.1, 4.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 136 – Examination results: OEV paragraph 20.2

Key	20.3
Requirement	All human resources must be acutely aware of the significance of information security. To this end, an education and training programme that is tailored to the tasks concerned must be devised and operated.
Observation	The *Richtlinie Informationssicherheit* document includes requirements for security training and awareness of the personnel involved in the e-voting processes. The cantons have a specific training programme aimed at all personnel involved in electronic voting. It includes a chapter dedicated to the security measures stated in the *Richtlinie Informationssicherheit* document.
Evidence	■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §2.4 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §3.4 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §3.4 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §3.4 ■ 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
Result	Pass
Finding	N/A
Relevance	N/A

Table 137 – Examination results: OEV paragraph 20.3

Physical and environment security

Key	21.1
Requirement	The security perimeters of the various premises of the infrastructure are clearly defined.
Observation	The *Hardware und Infrastruktur* document includes a chapter dedicated to the security of premises. The following concentric security perimeters are defined: ■ The cantons' buildings, ■ Offices/rooms, ■ Safes.
Evidence	■ 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 138 – Examination results: OEV paragraph 21.1

Key	21.2
Requirement	For physical entry to these various infrastructure premises, entry controls must be defined, implemented and appropriately checked.
Observation	The *Hardware und Infrastruktur* document lists the entry controls applicable to the physical security perimeters: ■ Buildings are protected by badges/keys, ■ Offices are protected by keys, ■ Safes are protected by split codes (to enforce the 4-eye principle).
Evidence	■ 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 139 – Examination results: OEV paragraph 21.2

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	The *Hardware und Infrastruktur* 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 *Richtlinie Informationssicherheit* document mentions that the electoral board monitors and has a right to audit the compliance with established rules regarding physical security.
Evidence	■ 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 140 – Examination results: OEV paragraph 21.3

Key	21.4
Requirement	All data must be processed and in particular stored exclusively in Switzerland.
Observation	On the cantons' side, the e-voting processes are executed in the premises of the cantons, on dedicated physical hardware. Processing and storage therefore take place in Switzerland only. The cantons publish information about e-voting on their web site. The canton of St. Gallen hosts its content management system (CMS) in a Swiss datacentre. The cantons of Graubünden and Thurgau hosts their web sites internally. The canton of Basel-Stadt hosts its cantonal CMS internally and its SharePoint servers externally, in Switzerland. In addition, the *Richtlinie Informationssicherheit* states that the transmission of e-voting data (cantons <-> Post, cantons <-> print offices) is performed exclusively on platforms located in Switzerland.
Evidence	■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.2 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.2 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.2 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 141 – Examination results: OEV paragraph 21.4

Management of communication and operations

Key	22.1
Requirement	Obligations and areas of responsibility must be apportioned so that the risks originating from human resources relating to operations and communications are reduced to residual risks that are compatible with the risk acceptance criteria.
Observation	At the cantons level, risks originating from human resources are mitigated by enforcing the 4-eye principle: All operations are carried out in presence of at least two people. In some cases, passwords are split among two or more people. Roles and responsibilities are clearly defined.
Evidence	■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §2.2.1, 3.6 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §3.2.1, 4.6 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §3.2.1, 4.6 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §3.2.1, 4.6
Result	Pass
Finding	N/A
Relevance	N/A

Table 142 – Examination results: OEV paragraph 22.1

Key	22.2
Requirement	Appropriate measures must be taken to protect against malware.
Observation	Protection against malware encompasses a wide range of measures, including user-awareness, end-point protection, management of removable media, rules for software installation, network segregation, patch management, hardening of components, ingress and egress IP communications filtering, content filtering, incident detection and response. The e-voting equipment under the cantons' responsibility is subject to hardening rules, patch management, limited incoming and outgoing communication from and towards trusted external systems, regular reinstallation / formatting, physical security measures. People in charge of the operation of the equipment are trained to follow well defined procedures. Incident management procedures are also available to deal with potential adverse events. In their risk assessment, the cantons estimate that risks associated to malware are low, given the current security controls in place. One of the controls listed in the assessment is the update of the malware signatures on the laptops before each ballot. In the examiners' opinion, the good practices adopted by the cantons to protect against malware seem appropriate to the context.
Evidence	BS, GR, SG, TG: E-Voting - Risikoportfolio, §P02-R02, P10-R02, P10-R13
Result	Pass
Finding	N/A
Relevance	N/A

Table 143 – Examination results: OEV paragraph 22.2

Key	22.3
Requirement	A detailed plan for data backup must be prepared and implemented. The data backup must be regularly reviewed to check that it is functioning correctly.
Observation	The backup strategy consists in saving data on a secure USB memory stick after each step of the process (Day 0, 1, 2, 3). The process for testing the restoration is defined in the test cases that are run after the delivery of a new version of the e-voting software and at least once a year.
Evidence	■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.5 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, § 4.5 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.5 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 144 – Examination results: OEV paragraph 22.3

Key	22.4
Requirement	Appropriate measures must be defined and implemented to protect the network from the threats listed in the risk assessment in accordance with Article 4 and in connection with Number 13 and for the security of network services.
Observation	From the cantons' perspective, networks are used to perform data exchanges, such as: ■ Connection to and synchronisation with the e-voting Admin-Portal, ■ Distribution of the register of voting cards to the municipalities, ■ Submission of test and control votes, ■ Distribution of the printing data to the print offices. Some threats mentioned in Number 13 may materialise through the exploitation of vulnerabilities at network level, e.g., man-in-the-middle attacks. Common good practices against such attacks include encrypting the data exchanged, applying network filtering and network segregation, hardening of network components, physical access control to cabling and network components. The *Richtlinie Informationssicherheit* document details the security measures applying to network components used in the context of electronic voting.
Evidence	■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8 ■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.3, 3.4, 3.11 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, §4.3, 4.4, 4.11 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.3, 4.4, 4.11 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4.3, 4.4, 4.11
Result	Pass
Finding	N/A
Relevance	N/A

Table 145 – Examination results: OEV paragraph 22.4

Key	22.5
Requirement	The procedures for using removable data carriers and for disposing of data carriers must be regulated in detail.
Observation	Removable data carriers are listed in the *Hardware und Infrastruktur* document. This document also describes how the data is securely deleted from the data carriers. The *Prozesse E-Voting* document also specifies at what moment the data carriers are deleted.
Evidence	■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §3.2 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §4.2 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §4.2 ■ TG: E-Voting -TG-Hardware-und-Infrastruktur – V1.5, §4.2 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 0.3.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 146 – Examination results: OEV paragraph 22.5

Allocation, administration and withdrawal of access and admission authorisations

Key	23.1
Requirement	It must be ensured that, during the ballot, any subsequent change in physical and logical access rights takes place only with the consent of the body responsible at cantonal level.
Observation	From the cantons' perspective, physical access rights in the context of e-voting include accesses to the buildings and offices wherefrom ballots are administered and to the safes where the infrastructure components are stored. Logical accesses include accesses to the e-voting infrastructure, as well as to the information portals dedicated to e-voting maintained by the cantons. Changes in general, and regarding access control in particular, are only allowed in case of emergency during a ballot. If any occur, those changes are recorded in the event log (*Ereignisbuch*).
Evidence	■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, §4.4 ■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.10 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, § 4.10 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.10 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4.10
Result	Pass
Finding	N/A
Relevance	N/A

Table 147 – Examination results: OEV paragraph 22.5

Key	23.2
Requirement	Access to infrastructure and software must be regulated and documented in detail on the basis of a risk assessment. In high-risk areas and for all manual operations in connection with the electronic ballot box (e.g. opening the voting channel, closing the voting channel, starting tallying), operations must be conducted by at least two persons. Manual operations in connection with the electronic ballot box (e.g. opening the voting channel, closing the voting channel, starting tallying) must be expressly authenticated.
Observation	The risk assessment performed by the cantons considers threats related to the unauthorised access to the e-voting infrastructure and software, as well as potential abuses of legitimate access rights. All operations in connection with the electronic ballot box are subject to the 4-eye principle and require authentication. The cantons maintain a logbook of the accesses performed in the context of an electronic ballot. The *Prozesse E-Voting* document mentions the step where people involved in the management of ballots choose passwords, use passwords and fill in the logbook (*Zugriff Safe*) when physically accessing the e-voting equipment. The document *Hardware und Infrastruktur* details the structure of the accounts used to authenticate to the computers involved in the e-voting operations.
Evidence	■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.7

	■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, § 4.7 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.7 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4.7 ■ BS: E-Voting BS - Hardware und Infrastruktur – V1.6, §4.3 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §5.3 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §5.3 ■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §5.3 ■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, steps 2.3, 2.8, 3.3.2, §4.4 ■ BS, GR, SG, TG: E-Voting - Risikoportfolio
Result	Pass
Finding	N/A
Relevance	N/A

Table 148 – Examination results: OEV paragraph 23.2

Key	23.3
Requirement	It must be guaranteed that information on the voting portal and related information pages cannot be changed without authorisation.
Observation	The cantonal e-voting management teams are in charge of voters information and responsible for the related communication artefacts published on their cantonal websites. An access control concept to the cantons' Content Management Systems ensures that only authorised personnel publish information.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §4 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §5 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §5 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §5
Result	Pass
Finding	N/A
Relevance	N/A

Table 149 – Examination results: OEV paragraph 23.3

Key	23.4
Requirement	During the ballot, access of any nature to the infrastructure that is of no relevance to the ballot must be prevented.
Observation	From the cantons' perspective, the e-voting infrastructure includes the cantonal computers (setup computer, tally computer, verifier computer, online computer, SRA computer), and data carriers. During the ballot, a formal step-by-step procedure is followed to ensure that only planned, authorised, relevant access to the infrastructure takes place. Access control is enforced to prevent from unlawful access.
Evidence	■ BS, GR, SG, TG: Prozesse E-Voting V1.8 ■ BS: Hardware und Infrastruktur V1.6, §3, 4.1.3 ■ GR: E-Voting - Hardware und Infrastruktur – V1.2, §4, 5.1.3 ■ SG: E-Voting - Hardware und Infrastruktur – V1.5, §4, 5.1.3

	■ TG: E-Voting-TG-Hardware-und-Infrastruktur – V1.5, §4, 5.1.3 ■ BS: E-Voting BS - Richtlinie Informationssicherheit – V1.6, §3.7 ■ GR: E-Voting - Richtlinie Informationssicherheit – V1.2, § 4.7 ■ SG: E-Voting - Richtlinie Informationssicherheit – V1.6, §4.7 ■ TG: E-Voting-TG-Richtlinie-Informationssicherheit – V1.6, §4.7
Result	Pass
Finding	N/A

Table 150 – Examination results: OEV paragraph 23.4

Key	23.5
Requirement	It must be ensured that none of the elements of the client-sided authentication credentials can be systematically intercepted, changed or redirected during transmission. For authentication, measures and technologies must be used that sufficiently minimise the risk of systematic abuse by third parties.
Observation	The cantons are responsible for generating the polling cards (and therefore the voters' authentication credentials), having them printed by the print offices and distributed by post to the voters. The transmission of the voting cards occurs through secure channels (see Number 7.1). Once printed out, the polling cards are packaged by the print offices and collected by the Post for distribution. The technology used for the authentication of voters is under the responsibility of the e-voting system provider.
Evidence	BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8 steps SRA-1, SRA-2, SRA-3
Result	Pass
Finding	N/A
Relevance	N/A

Table 151 – Examination results: OEV paragraph 23.5

Development and maintenance of information systems

Reliable and verifiable compilation and deployment

Key	24.3.5
Requirement	The quality of the evidence of reliable and verifiable compilation and reliable and verifiable deployment must be confirmed by the presence of at least two witnesses from different institutions or by technical procedures to establish the truth of the evidence in the light of current academic knowledge and experience.
Observation	To meet this requirement, the cantons perform a Trusted Build of the e-voting system software from the official audited source code made available by Swiss Post, and confirm that the resulting hash values match those published by Swiss Post. In addition, an independent expert is mandated to carry out the same process.

	When deploying the software components on their infrastructure, the cantons verify the integrity of each file by comparing its hash value against the results of their own Trusted Build. For the scripts whose source code is not publicly disclosed by the Post, the verification is limited to a comparison against known-good hashes provided by the Post. This entire process is conducted in accordance with the four-eyes principle, ensuring that at least two independent parties validate the integrity of the build and deployment.
Evidence	■ BS, GR, SG, TG: E-Voting - Prozesse E-Voting - V1.8, step 0.3.4 ■ https://rechtsdienst.tg.ch/public/upload/assets/170210/241117_E-Voting-System_Post_release_1.4.4.4_Trusted_Build_Bericht_TG_SG_BS_GR.pdf?fp=1 ■ https://www.442security.com/TrustedBuild-eVoting.html
Result	Pass
Finding	N/A
Relevance	N/A

Table 152 – Examination results: OEV paragraph 24.3.5

Key	24.3.6
Requirement	The chain of evidence of reliable and verifiable compilation and deployment is made publicly available.
Observation	The *Konzept Information der Stimmberechtigten* document mentions that the hashes of the artefacts from the Trusted Build and Deployment processes are made publicly available on the cantons' website and e-voting landing page.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §8.2 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §9.2 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §9.2 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §9.2 ■ BS: https://bs.evoting.ch/ ■ GR: https://gr.evoting.ch/ ■ SG: https://sg.evoting.ch/ ■ TG: https://tg.evoting.ch/
Result	Pass
Finding	N/A
Relevance	N/A

Table 153 – Examination results: OEV paragraph 24.3.6

Systematic correction of flaws

Key	24.4.1
Requirement	Processes are defined for the correction of flaws. The processes include: ■ documentation of specific aspects, in particular with regard to the traceability of flaws for all versions of the software, and of the methods used to ensure that system users have information on flaws, corrections and possible corrective actions;

	■ the obligation to describe the nature and impact of all security flaws, information on the status of work to find a solution and the corrective measures adopted; ■ a description of how system users can make reports and enquiries about suspected flaws in the software known to the software developers; ■ a procedure requiring a timely response and automatic dispatch of security flaw reports and appropriate corrective actions to registered system users who may be affected by the flaw.
Observation	The *Konzept Information der Stimmberechtigten* document mentions that known flaws are transparently communicated to the e-voting system users. They are published on the Post's source code repository site as well as on its community website. The cantons reference those two information sources on their website. The Post is responsible for the correction of flaws itself as well as for the detailed content of the vulnerability reports.
Evidence	■ BS: E-Voting BS - Konzept Information der Stimmberechtigten – V1.5, §8.3 ■ GR: E-Voting - Konzept Information der Stimmberechtigten – V1.3, §9.2 ■ SG: E-Voting - Konzept Information der Stimmberechtigten – V1.5, §9.2 ■ TG: E-Voting-TG-Konzept-Information-der-Stimmberechtigten – V1.5, §9.2 ■ https://gitlab.com/groups/swisspost-evoting/-/issues
Result	Pass
Finding	N/A
Relevance	N/A

Table 154 – Examination results: OEV paragraph 24.4.1

Learnability

Key	25.6.2
Requirement	Persons who operate and use the system must be trained and provided with the necessary documentation.
Observation	The cantons have a training program for all people operating the system: ■ Members of the Electoral-Board, ■ Members of the Admin-Board. A mandatory training takes place 2-3 months before each ballot and a short refresher occurs at the start of the second (D2) and third days (D3) of each ballot. Instructions on e-voting and on e-voting security are also provided to the communes (in the cantons where communes are involved in e-voting) and to the print offices.
Evidence	■ 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
Result	Pass
Finding	N/A
Relevance	N/A

Table 155 – Examination results: OEV paragraph 25.6.2

Key	25.6.3
Requirement	Training includes the opportunity to train on a system designed for training purposes.
Observation	The document *Konzept Schulungen und interne Information* mentions that the members of the Admin-Board gain routine and experience through several test runs before the first ballot and ballot tests before each subsequent ballot. It is ensured that the persons concerned have access to the intended test environment and are provided with the necessary documentation from Swiss Post and the canton to assist them.
Evidence	■ BS: E-Voting BS - Konzept Schulungen und interne Information – V1.1, §1 ■ GR: E-Voting - Konzept Schulungen und interne Information – V1.1, §2 ■ SG: E-Voting - Konzept Schulungen und interne Information – V1.1, §2 ■ TG: E-Voting-TG-Konzept-Schulungen-und-interne-Information – V1.1, §2
Result	Pass
Finding	N/A
Relevance	N/A

Table 156 – Examination results: OEV paragraph 25.6.3

Key	25.6.4
Requirement	Help on using the system must be readily available.
Observation	All participants to the training receive a set of documentation about how to use the system.
Evidence	■ BS: E-Voting BS - Konzept Schulungen und interne Information – V1.1, §1.1 ■ GR: E-Voting - Konzept Schulungen und interne Information – V1.1, §2.1 ■ SG: E-Voting - Konzept Schulungen und interne Information – V1.1, §2.1 ■ TG: E-Voting-TG-Konzept-Schulungen-und-interne-Information – V1.1, §2.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 157 – Examination results: OEV paragraph 25.6.4

5 Summary of findings and recommendations

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

Key	Art. 11
Requirement	**Disclosure of the source code and of the documentation on the system and its operation** 1 The canton shall ensure that the following documents are published: 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. 2 The following need not be published: 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.
Finding	The source code of the VPCS software, which is used to generate polling cards in Basel-Stadt, Graubünden, and Thurgau, as well as the source code of the associated helper scripts, has not been published. The publication of the VPCS software's source code is planned for May 2025.
Recommendation	The cantons should require the Post to publish the source code of the helper scripts to enforce the principle of transparency.

Table 158 – Finding related to Art. 11

Key	15.1
Requirement	Electronic certificates must be managed according to the best practices.
Finding	The cantons do not provide any detail regarding the “best practices” in place to manage certificates used on the informational cantonal websites dedicated to e-voting.
Recommendation	The best practices regarding the management of the said certificates should be described in details (e.g., generation, distribution, protection of private keys, revocation, renewal, etc.)

Table 159 – Finding related to requirement 15.1

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.
Finding	The examiners did not receive any evidence that the electronic certificates used for data signature originate from a recognised supplier of certificate services under the ESigA.
Recommendation	The need to use certificates that have been issued by a recognised supplier of certificate services under the ESigA does not seem to be justified from an information security standpoint for some of the use cases of the cantons. When installed on an offline device, it is not possible to check the Certificate Revocation List (CRL) of the corresponding issuing certificate authority, which runs contrary to good practices in terms of qualified certificate management. Moreover, suppliers of ESigA certificates do not seem to supply signing certificates for machines. Therefore, the cantons should ask for a derogation from the Federal Chancellery to continue their current practice.

Table 160 – Finding related to requirement 15.4

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 Comittee 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. [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. [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].