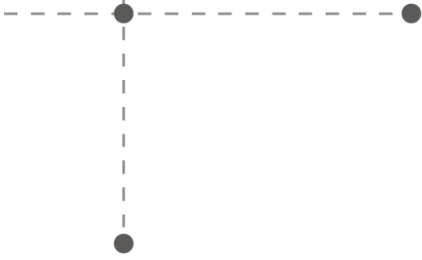




Cyberdefense



Federal Chancellery

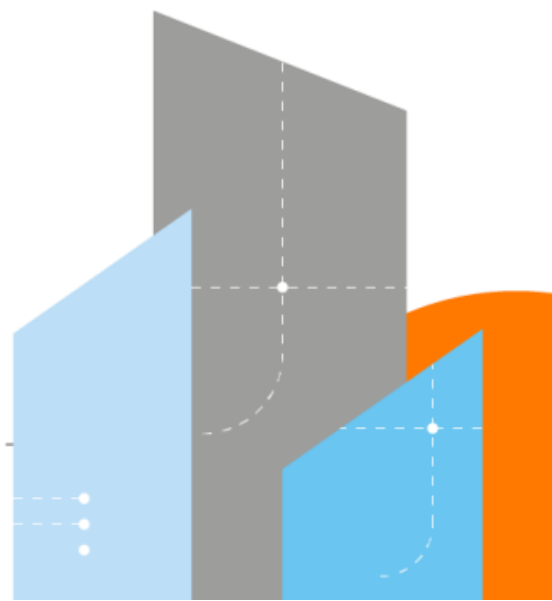
Examination of the Swiss Internet voting system

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

16 December 2025



Orange Restricted



Contact information

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

Contributor

Name	Date
Stéphane Adamiste	Chief Product Officer, Orange Cyberdefense Switzerland

Document history

Version	Date	Authors	Change details
0.1	2024/08/18	Stéphane Adamiste	Working version
0.9	2025/11/27	Stéphane Adamiste	Release candidate
1.0	2025/12/16	Stéphane Adamiste	Valid version

Contents

1	Context	8
2	Methodology	10
	2.1 Process	10
	2.2 Audit scope definition	10
	2.3 Collection of evidence	10
	2.4 Findings	11
	2.5 Classification of findings	11
	2.6 Relevance of the assessment criteria	11
	2.7 Assumptions	11
3	Examination criteria	12
4	Examination results	25
5	Summary of findings and recommendations	76
6	References	78

Management summary

Context, scope and objective of the examination

Following several audits performed over the last years (first full audit, follow-up audits of the initial findings, audit of changes), the objective of this examination was to fully re-assess to which extent the Swiss Post's infrastructure and organisational measures supporting its e-voting system satisfies a subset of requirements (audit concept v1.6, scope 3 - *Infrastructure and operation, b) Assess the infrastructure and organisational measures of the system provider*) set forth by the Federal Chancellery's Ordinance on Electronic Voting. In total, the examination included 124 criteria.

Methodology

The examiners looked for evidence of effort to comply with said criteria by performing interviews of Swiss Post personnel in charge of the setup and operation of the e-voting system's infrastructure, and by analysing the related documentation (i.e., policies, procedures, specifications, reports, processes, etc.). A visit to the datacentre infrastructure hosting the e-voting components operated by Swiss Post also took place. The examination was performed during the months of September and October 2025.

Results

Overall, Swiss Post has demonstrated a high level of compliance with the applicable requirements of the Ordinance on Electronic Voting.

During the audit, two non-conformities were identified regarding physical access to the control components, as detailed below:

Key	Requirement	Finding
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).	During their on-site visit to one of the data centres hosting the control components (on September 17th), the examiners observed that the four-eyes principle had not been applied during the last physical interventions on the control components, as only one name appeared in the corresponding logs.
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: <ul style="list-style-type: none">■ 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.	During their on-site visit (on September 17 th), a lack of segregation of duties was observed within the team: all six members had access to all four control components.

	<ul style="list-style-type: none"> ■ The control components should be connected to different local networks. <p>A control component must take the form of a physical device. Virtualisation across multiple physical devices is not permitted.</p>	
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Table 1 – Findings related to the physical access to the control components

Swiss Post initiated a corrective action plan to address these issues:

- Number 3.14: The new procedure, effective since October 7th, now requires all physical interventions to be performed under supervision: personnel physically accessing the control components do not know the codes to the safes where the keys to the equipment racks are stored and are therefore unable to gain access unaccompanied.
- Number 3.15: Each control component is housed in its own rack with a unique lock, and the rack keys are stored separately in dedicated safes.

The examiners have been provided with a comprehensive report on the implementation of the action plan (*2025-12-02_Protokoll-physischer-Umbau-CC-Infrastruktur*), which confirms that the observed non-conformities have been addressed.

Besides, three additional non-conformities were identified, which result from a strict, literal interpretation of the ordinance. They are presented in the following table.

Key	Requirement	Finding
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 a certificate that has been issued by a recognised supplier of certificate services under the ESigA.	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.
21.4	All data must be processed exclusively in Switzerland, including storage.	The source code of the e-voting system as well as all the related documentation are hosted on the GitLab source code repository in the USA.
24.2.1	<p>An operating manual is created that includes the following for each user role:</p> <ul style="list-style-type: none"> ■ a description of the functions that the user can access and the permissions that must be controlled in a secure environment, including appropriate warnings; ■ a description of how the available interfaces can be used in a secure manner; ■ a description of the available functions and interfaces, in particular all security parameters under the control of the user, highlighting the values relevant to security; ■ a precise description of all types of security events related to the user-accessible functions to be 	Swiss Post's operating manual does not include a role-function matrix specifying which functionalities are accessible to each type of user, nor does it provide a structured overview of all security-relevant events associated with user-accessible functions.

	<p>performed, including adjustments to the security properties of elements under the control of the security functions;</p> <ul style="list-style-type: none"> ■ a description of the security measures to be implemented in order to achieve the operational security objectives. 	
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

Table 2 – Findings related to Numbers 15.4, 21.4, 24.2.1

However, when assessed in the broader context of information security and operational feasibility, the identified gaps do not necessarily indicate a material weakness nor a security-relevant deficiency.

The rationale for this position is summarised below for each requirement.

- Number 15.4: The certificates used for these signatures are generated autonomously by each component according to the Direct Trust Model introduced with version 1.3 of the system. Under this model, trust is established directly between the communicating components through the controlled exchange of self-generated certificates, rather than through a recognised ESigA certificate authority. This approach is consistent with the technical constraints of the e-voting system, particularly for components operating offline, where checking certificate revocation lists is not feasible. In addition, suppliers of ESigA-compliant certificates generally do not provide machine-signing certificates suitable for these use cases. The Federal Chancellery has explicitly authorised the Direct Trust approach for the cantons, making this deviation compliant at the regulatory level. Although it does not meet the literal wording of requirement 15.4, the model is formally accepted and does not introduce any relevant security risk.
- Number 21.4: Swiss Post interprets the expression “all data” as referring exclusively to data directly linked to voting events (e.g., voter data, encrypted ballots, verification material, audit-relevant records, etc.) Under this interpretation, ancillary material such as source code, technical documentation, and development artefacts does not fall within the scope of the requirement. During previous audits, Swiss Post has already confirmed that it does not intend to migrate the hosting of its source code or documentation away from GitLab. Although the requirement is not met under a strict literal reading, the deviation has no material impact on the security or trustworthiness of the voting process. No corrective action is required in the examiners’ opinion.
- Number 24.2.1: From a practical perspective, achieving full alignment with the literal wording of the requirement would likely reduce the document’s usability, as the operational guide is designed to be procedural and actionable rather than an exhaustive reference document. In the examiners’ opinion, the current level of detail is therefore consistent with the document’s operational purpose, while still supporting secure execution of all described tasks.

Recommendations

No recommendations are issued as part of this audit. The identified non-conformities have either been fully addressed by the corrective action plan or do not require further

remediation based on their limited security relevance and the examiners' assessment.

Final note

The examiners conclude this summary by thanking the involved Swiss Post personnel for their cooperation and for the transparency demonstrated throughout the duration of 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. SCRT, now Orange Cyberdefense Switzerland (“OCD CH”) was mandated by the Federal Chancellery to assess the compliance of the Swiss Post’s revamped e-voting system against some of the requirements of the draft OEV. One of the examination scopes covered by SCRT was defined as follows in the audit concept: Scope 3: *Infrastructure and operation, b) Assess the infrastructure and*

organisational measures of the system provider. The audit report was published in April 2022 on the Federal Chancellery's website [6]

7. In May 2022, the Federal Council enacted the partially revised Ordinance on Political Rights (PoRo) [7], which became applicable from July 1st 2022. The totally revised Federal Chancellery Ordinance on Electronic Voting (OEV) [8] came into force on the same date.
8. In September 2022, an updated version of the audit concept was issued by the Federal Chancellery [9].
9. A second assessment was conducted in mid-September 2022 to follow-up on the findings raised in the initial audit report. The audit report was published in March 2023 on the Federal Chancellery's website [10].
10. A third assessment was conducted in April 2023 to follow-up on the findings raised in the second audit report and to consider changes into the Post's infrastructure, as well as criteria added by the Federal Chancellery to the 3 b) scope [11].
11. In 2024, OCD CH assessed the impact of a change initiated by the Post on its infrastructure (i.e., the improvement of access control to the control components through the implementation of jump hosts) on the overall compliance level with the requirements of the OEV [12].
12. In February 2025, an updated version of the audit concept was issued by the Federal Chancellery [13]
13. The present assessment consists of full re-assessment of the e-voting system operated by the Swiss Post against the criteria forming scope 3b).

2 Methodology

2.1 Process

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

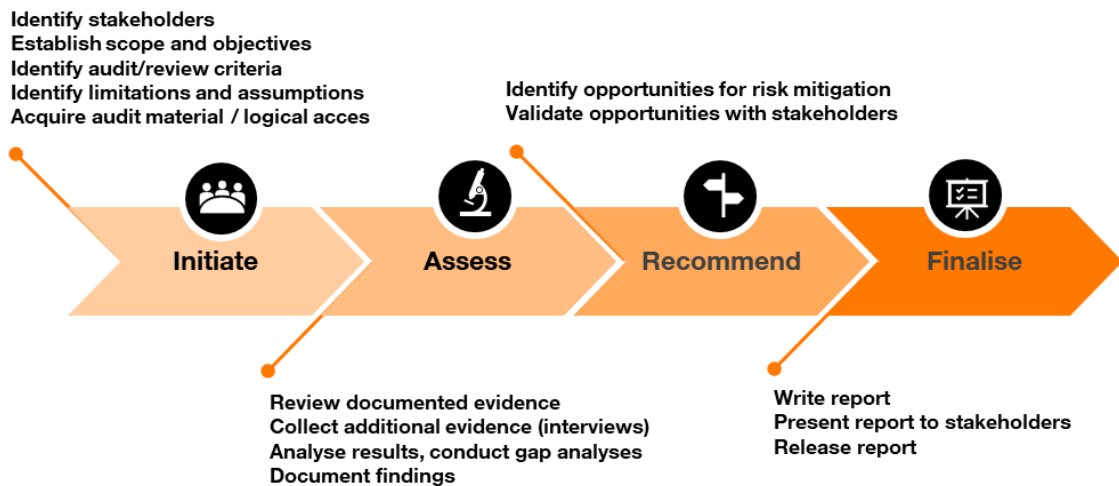


Figure 1: Examination process

2.2 Audit scope definition

15. The examiners assessed compliance of the auditee with *audit scope 3 – Infrastructure and operation, item b*, i.e., the infrastructure and organisational measures of the system provider. The applicable evaluation criteria are those defined in the *Audit concept v1.6 for examining Swiss internet voting systems* [13].

16. The OEV provides the following definitions of “operation” and “infrastructure” which further clarify the scope of the assessment:

- “*Operation* means any action, including maintenance, with a technical, administrative or legal aspect and related management activities, carried out by a canton, system operator or printing office that are required to conduct electronic ballots”;
- “*Infrastructure* means hardware, software of third-party components in accordance with Article 11 paragraph 2 letter a, network elements, premises, services and equipment of any nature at any operating bodies that are required for the secure operation of electronic voting”.

2.3 Collection of evidence

17. 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.

2.4 Findings

18. 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).

2.5 Classification of findings

19. 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.

20. 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.

2.6 Relevance of the assessment criteria

21. 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.

2.7 Assumptions

2.7.1 Trustworthiness of statements

22. The examiners assume that the examinees were honest and transparent when providing answers to the examiners' assessment questions. The direct observation of the actual implementation of the OEV's requirements within the e-voting system was limited to the visit to one of the datacentre rooms hosting the control components of the e-voting system.

2.7.2 Enforcement of security measures

23. 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. As with the previous assumption, the observation of the system's actual implementation was limited to the visit to one datacentre room hosting the control components.

3 Examination criteria

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

Cryptographic protocol requirements for complete verifiability

Key	Requirement
2.5	<p>Requirement for the cryptographic protocol: individual verifiability</p> <p>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</p> <ul style="list-style-type: none"> ■ 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	<p>Requirement for the cryptographic protocol: universal verifiability</p> <p>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:</p> <ul style="list-style-type: none"> ■ after the votes were registered as cast in conformity with the system, has altered or misappropriated any partial votes before the result was determined; ■ has inserted any votes or partial votes not cast in conformity with the system which were taken into account in determining the result.
2.7	<p>Requirements for the cryptographic protocol: preserving voting secrecy and excluding premature partial results</p>
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.
2.9	<p>List of trustworthy and untrustworthy system participants</p>
2.9.1.2	<p>For soundness of the proofs referred to in Number 2.5</p> <p>The following system participants may be considered trustworthy:</p> <ul style="list-style-type: none"> ■ set-up component ■ print component ■ one of four control components per group, leaving open which one it is
2.9.2.2	<p>For soundness of the proofs referred to in Number 2.6</p> <p>The following system participants may be considered trustworthy:</p> <ul style="list-style-type: none"> ■ 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	<p>For preserving voting secrecy and excluding premature partial results in accordance with Number 2.7</p> <p>It may be assumed that trustworthy channels exist to distribute electronic certificates among system participants. Number 3.8 applies.</p>
2.9.4.2	<p>For the effectiveness of the authentication referred to in Number 2.8</p>

Key	Requirement
	The following system participants may be considered trustworthy: <ul style="list-style-type: none"> ■ set-up component ■ print component ■ one of four control components per group, leaving open which one it is
2.13	Requirements for the definition and description of the cryptographic protocol
2.13.3	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

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

Key	Requirement
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, a published reference must be used for all programs to check whether 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	Trustworthy components may not be connected to the internet when installing or updating software.
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.
3.14	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: <ul style="list-style-type: none"> ■ 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.

Key	Requirement
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
3.19	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

Information and instructions

Key	Requirement
8.13	Known flaws and the need for action associated with them are communicated transparently

Table 5 - E-voting requirements: Information and instructions

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.
11.4	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.

Table 6 - 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 premature results to be determined.
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 7 - E-voting requirements: Confidential data

Threats

Key	Requirement																														
13.1	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.																														
13.2	<p>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</p> <table border="1"> <thead> <tr> <th></th> <th>Description</th> <th>Security objective concerned (in accordance with Art. 4 para. 3)</th> </tr> </thead> <tbody> <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)¹.</td> <td>Accuracy of the result</td> </tr> <tr> <td>13.5</td> <td>An external attacker changes vote using the man-in-the-middle (MITM) technique².</td> <td>Accuracy of the result</td> </tr> <tr> <td>13.6</td> <td>Using MITM, an external attacker sends maliciously altered data that are necessary to cast a vote and that originate in the online system (e.g. Javascript files).</td> <td>Accuracy of the result</td> </tr> <tr> <td>13.7</td> <td>An internal attacker manipulates the software, causing it not to store the votes.</td> <td>Accuracy of the result</td> </tr> <tr> <td>13.8</td> <td>An internal attacker changes, deletes or duplicates the votes</td> <td>Accuracy of the result</td> </tr> <tr> <td>13.9</td> <td>An internal attacker inserts votes.</td> <td>Accuracy of the result</td> </tr> <tr> <td>13.10</td> <td>A hostile organisation infiltrates the system with the aim of falsifying the result.</td> <td>Accuracy of the result</td> </tr> <tr> <td>13.11</td> <td>An internal attacker copies voting papers and uses them.</td> <td>Accuracy of the result</td> </tr> </tbody> </table>		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) ¹ .	Accuracy of the result	13.5	An external attacker changes vote using the man-in-the-middle (MITM) technique ² .	Accuracy of the result	13.6	Using MITM, an external attacker sends maliciously altered data that are necessary to cast a vote and that originate in the online system (e.g. Javascript files).	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, deletes or duplicates 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
	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) ¹ .	Accuracy of the result																													
13.5	An external attacker changes vote using the man-in-the-middle (MITM) technique ² .	Accuracy of the result																													
13.6	Using MITM, an external attacker sends maliciously altered data that are necessary to cast a vote and that originate in the online system (e.g. Javascript files).	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, deletes or duplicates 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																													

¹ Also known as DNS poisoning. This is an attack which successfully falsifies the correlation between a host name and the related IP address.

² 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	
	13.12 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 manipulates the set-up components or steals security-relevant data.	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 backdoor ³ 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

³ 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.

Key	Requirement		
	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	An internal attacker manipulates the software to reveal the votes	Preservation of voting secrecy and exclusion of premature results
	13.29	Malware on the user device makes voting impossible.	Accessibility and operability of the voting system
	13.30	A hostile organisation carries out a denial-of-service (DOS) ⁴ attack.	Accessibility and operability of the voting system
	13.31	An internal attacker carries out an incorrect configuration; it does not get to the tallying.	Accessibility and operability of the voting system
	13.32	An internal attacker falsifies the cryptographic proofs of universal verifiability.	Accessibility and operability of the voting system
	13.33	A technical error in the system causes the system to be unavailable at the time of the tallying.	Accessibility and operability of the voting system
	13.34	One of the auditors' technical aids does not work at the time of tallying.	Accessibility and operability of the voting system
	13.35	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
	13.36	An internal attacker steals voters' address data.	Protection of personal information relating to voters
	13.37	Malware influences voters' opinions.	Protection of information intended for voters from manipulation

⁴ In digital data processing, this is the non-availability of a service that should be available.

Key	Requirement	
	13.38	An internal attacker manipulates the information website or voting portal and thereby deceives voters. Protection of information intended for voters from manipulation
	13.39	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
	13.40	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 8 - E-voting requirements: Threats

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

Key	Requirement
14.1	<p>An infrastructure monitoring system detects incidents that could endanger the security, including availability, of the system and alerts the responsible personnel. The personnel deal with incidents according to a predetermined procedure. Crisis scenarios and rescue plans serve as guidelines (and include a plan that guarantees that voting-related activities can continue) and are applied as required.</p> <p>Errors in the registration of votes in the control components and in the ballot box must be detected. Further information relating to the error must be available in order to identify and eliminate the cause. Any incidents detected must be reported to the body responsible at cantonal level.</p>
14.2	<p>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.</p> <p>The content of the records covers at least the following events:</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>The system logs are made available to the body responsible at cantonal level in such a way that it can interpret the information.</p>
14.3	<p>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.</p>

Key	Requirement
	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 ensure voting secrecy
14.5	It must be guaranteed that in the event of a malfunction, the votes and the data that prove the smooth operation of the vote tallying are stored safely in the infrastructure.
14.6	After a breakdown in the system or a failure of communication or storage media, the system enters a recovery mode in which it is possible to return to a safe state. Voting processes that have been started are interrupted. The person voting cannot resume voting until the system is returned to a secure state.
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 9 - 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.
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 ⁵ on Electronic Signatures (ESigA). The signature must be verified by means of a certificate that has been issued by a recognised supplier of certificate services under the ESigA.

Table 10 - 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	The systems must be protected against attack (irrespective of the nature of the attack or of its

⁵ SR 943.03

Key	Requirement
	origin).

Table 11 - 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 irrespective of type, such as suppliers, service providers, etc.) 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 12 - E-voting requirements: Organisation of information security

Management of non-material and material 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 non-material and material 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 13 - E-voting requirements: Management of non-material and material 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	Human resources managers must accept full responsibility for guaranteeing the trustworthiness of human resources.
20.3	All human resources must be acutely aware of the need for information security. To this end, an education and training programme that is tailored to the tasks concerned must be devised and operated.

Table 14 - 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 exclusively in Switzerland, including storage.

Table 15 - E-voting requirements: Management of communication and operations

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.
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 16 - 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 to the infrastructure of any nature 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

Key	Requirement
	abuse by third parties.

Table 17 - E-voting requirements: Allocation, administration and withdrawal of access and admission authorisations

Development and maintenance of information systems

Key	Requirement
24.2.1	<p>An operating manual is created that includes the following for each user role:</p> <ul style="list-style-type: none"> ■ a description of the functions that the user can access and the permissions that must be controlled in a secure environment, including appropriate warnings; ■ a description of how the available interfaces can be used in a secure manner; ■ a description of the available functions and interfaces, in particular all security parameters under the control of the user, highlighting the values relevant to security; ■ a precise description of all types of security events related to the user-accessible functions to be performed, including adjustments to the security properties of elements under the control of the security functions; ■ a description of the security measures to be implemented in order to achieve the operational security objectives.
24.2.2	The operating manual must identify all possible modes of operation of the software, including the resumption of operation after the detection of errors and the description of the consequences and effects of errors on the maintenance of secure operation
24.2.3	The operating manual must be precise and fit for purpose.
24.3.1	<p>The preparation process describes all the steps necessary for:</p> <ul style="list-style-type: none"> ■ the secure acceptance of the system components in accordance with the delivery procedure; ■ the secure preparation of the operating environment in accordance with the operational security objectives; ■ the secure installation of the software in the operating environment.
24.3.2	The delivery of the software or parts of the system must be documented and include all processes required to maintain security in the delivery of the software
24.3.3	<p>A reliable and verifiable compilation with appropriate security measures must be carried out. This ensures that the executable code is a verifiable and faithful representation of the source code which has been subjected to public scrutiny and independent examinations. The compilation allows a chain of proofs to be created for the verification of the software and includes in particular:</p> <ul style="list-style-type: none"> ■ evidence that the compilation environment is designed as described on the public platform (all tools with the respective version, operating system and any configurations); any derogations must be documented and justified; ■ evidence that the software has been compiled in accordance with the instructions available on the public platform; if an error in the instructions is found during compilation, this must be recorded and the documentation must subsequently be corrected; ■ evidence that the source code submitted for public scrutiny and examined is in fact the source code used for compilation; ■ evidence that no elements other than those provided for in the instructions have been introduced; ■ evidence that the cryptographic signature of all dependencies has been verified against a proven, public, and trusted reference (e.g. Maven Central Repository); ■ evidence that a dependency vulnerability analysis has been performed and that, if vulnerabilities relevant to the software exist, they do not render the software vulnerable to

Key	Requirement
	<p>attack;</p> <ul style="list-style-type: none"> ■ evidence that the parameters introduced, if any, do not render the system vulnerable.
24.3.4	<p>A reliable and verifiable deployment with appropriate security measures must be carried out. This is to ensure that:</p> <ol style="list-style-type: none"> 1. the code used in production is a verifiable and faithful representation of the source code which has been subjected to public scrutiny and independent examinations; and 2. the production environment conforms to that which has been subjected to public scrutiny and independent examinations. <p>The deployment allows a chain of proofs to be created for the verification of the software and includes in particular:</p> <ul style="list-style-type: none"> ■ evidence that the production environment is the same as that which has been subjected to public scrutiny and independent examinations; any discrepancies (firmware version, configuration files, etc.) must be documented and justified; ■ evidence that the software deployed in the production environment is in fact that which was created using a reliable and verifiable compilation process; ■ evidence that the parameters introduced, if any, do not render the system vulnerable.
24.3.5	<p>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 scientific knowledge and experience</p>
24.3.6	<p>The chain of evidence of reliable and verifiable compilation and deployment is made publicly available</p>
24.4.1	<p>Processes are defined for the correction of flaws. The processes include:</p> <ul style="list-style-type: none"> ■ 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.
24.4.2	<p>A process is defined for handling reported flaws.</p> <p>This process ensures that all reported and confirmed flaws are corrected and that the procedures for correction are communicated to system users.</p> <p>It provides for arrangements to ensure that the correction of security flaws does not give rise to new security flaws.</p>
24.4.3	<p>Policies must be defined for the reporting and correction of flaws. These include:</p> <ul style="list-style-type: none"> ■ instructions on how system users can report suspected security flaws to the developer; ■ instructions on how system users can register with the developer to receive reports of security flaws and the corrections; ■ details of specific contact points for all reports and inquiries on security issues concerning the software.

Table 18 - E-voting requirements: Development and maintenance of information systems

Operation

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 19 - E-voting requirements: Operation

4 Examination results

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

Requirement for the cryptographic protocol: individual verifiability

Key	2.5
Requirement	<p>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</p> <ul style="list-style-type: none"> ■ 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.
Observation	<p>Article 5 paragraph 2 defines the requirements for <i>individual verifiability</i>, i.e., that voters must receive proofs allowing them to verify that their vote has been correctly registered as cast and that no vote has been maliciously cast on their behalf. Article 6 specifies that the soundness of these proofs relies on the trustworthiness of the <i>trustworthy part of the system</i> (letter a) and on the procedure for generating and printing the voting papers (letter b).</p> <p>The correctness of the cryptographic protocol implementing these proofs, as well as the assurance that these properties are fulfilled, are outside the scope of the present audit and are subject to dedicated cryptographic and protocol assessments.</p> <p>From an infrastructure and operations perspective, Swiss Post applies a comprehensive range of security assurance measures to ensure that the components and processes necessary to deliver individual verifiability proofs be operated in a secure, controlled, and monitored environment. <i>The Security Whitepaper of the Swiss Post Voting System</i> document lists the following practices in relation to infrastructure and operations:</p> <ul style="list-style-type: none"> ■ Application of threat modelling techniques to identify threats relating to the e-voting system and corresponding risk mitigation measures in a systematic manner; ■ Secure operational processes for software development and deployment, including a trusted build pipeline and release management procedures documented in a public GitLab repository, ensuring that the code executed in production corresponds to the reviewed and published source code; ■ Continuous external testing, including a public bug bounty program and regular Public Intrusion Tests (PITs), whose results are published and integrated into the operational security process; ■ Operation under an ISO/IEC 27001:2022-certified ISMS, covering infrastructure and processes relevant to e-voting. <p>The <i>Infrastructure Whitepaper</i> provides details on the security measures implemented at the infrastructure level to mitigate threats and ensure the integrity and availability of the system. In particular, it describes the implementation and operation of the <i>trustworthy part of the system</i>, which consists of multiple independent control components. These are deployed in separate environments, operated under separation-of-duties principles, and continuously monitored, such that misuse can be detected even if only one component functions correctly.</p> <p>These measures provide assurance that the infrastructure and operational environment underpinning the Swiss Post voting system support the availability, integrity, and trustworthiness of the individual verifiability mechanisms.</p>
Evidence	<ul style="list-style-type: none"> ■ Security Whitepaper of the Swiss Post Voting System

	<ul style="list-style-type: none"> ■ Infrastructure Whitepaper of the Swiss Post Voting System
Result	Pass
Finding	N/A
Relevance	While Article 6 OEV explicitly bases the soundness of proofs on the trustworthiness of the trustworthy part of the system (letter a) and the procedure for generating and printing the voting papers (letter b), in practice, additional dependencies arise. First, the secure distribution of voting papers to voters is a prerequisite for the reliability of the return-code mechanism. Second, the organisational channel by which voters request proofs from the canton (typically by telephone) also becomes a critical dependency. If this channel does not include robust procedures for mutually authenticating the voter and the authorised canton staff, and for reliably accessing the relevant system logs, the credibility of the individual verifiability proof under Article 5 paragraph 2 letter b may be weakened.

Table 20 – Examination results: OEV paragraph 2.5

Requirement for the cryptographic protocol: universal verifiability

Key	2.6
Requirement	<p>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:</p> <ul style="list-style-type: none"> ■ after the votes were registered as cast in conformity with the system, has altered or misappropriated any partial votes before the result was determined; ■ has inserted any votes or partial votes not cast in conformity with the system which were taken into account in determining the result.
Observation	<p>Article 5 paragraph 3 letter a defines the requirements for universal verifiability, i.e., that auditors receive proofs allowing them to verify that no attacker has altered or misappropriated any partial votes after they were registered as cast, and that no votes or partial votes not cast in conformity with the system have been introduced into the tally. Article 6 specifies that the soundness of these proofs relies on the trustworthiness of the trustworthy part of the system (letter a) and on the technical aids used by the auditors for the audit (letter c).</p> <p>The correctness of the cryptographic protocol implementing these proofs, as well as the assurance that these properties are fulfilled, are outside the scope of the present audit and are subject to dedicated cryptographic and protocol assessments.</p> <p>In the context of universal verifiability, the measures detailed in the audit observation for §2.5 here above specifically ensure that the components responsible for storing and tallying votes are operated in a secure, controlled, and monitored environment, thereby supporting the integrity of the proofs provided to auditors.</p> <p>These measures provide assurance that auditors can rely on the infrastructure and operations of the Swiss Post voting system to obtain sound proofs of universal verifiability.</p>
Evidence	<ul style="list-style-type: none"> ■ Security Whitepaper of the Swiss Post Voting System ■ Infrastructure Whitepaper of the Swiss Post Voting System
Result	Pass
Finding	N/A
Relevance	N/A

Table 21 – Examination results: OEV paragraph 2.5

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	<p>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.</p> <p>The Post has conducted a security analysis of the said cryptographic protocol (See <i>Swiss Post voting protocol computational proof</i> document) 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.</p> <p>From an infrastructure point of view, an attacker aiming to breach voting secrecy and establish premature results without controlling the voters or their user devices would likely try to execute one of the following threat scenarios:</p> <ul style="list-style-type: none"> ■ Introduction of a backdoor in the system via a software dependency; ■ Introduction of malicious code into the e-voting software directly; ■ Manipulation of the e-voting software; ■ Redirection of votes using DNS spoofing; ■ Reading of votes using man-in-the-middle attacks; ■ Abuse of the decrypting key to reveal votes; ■ Exploitation of a weakness in the encryption process. <p>Those scenarios have been taken into account by the Post in its Information Security and Data Privacy concept and have been subject to risk mitigation measures, as required by Number 13.1.</p> <p>In this regard, the document <i>POST.DS6_Risikenauszug.Kantone_</i> maps the threats listed above with the main associated ISO27002 mitigating controls.</p> <p>The adequate implementation of those controls, as stated by the auditors across the present audit report, proves to reduce risks of breaching voting secrecy or establishing premature results to a residual level.</p>
Evidence	<ul style="list-style-type: none"> ■ Swiss Post voting protocol computational proof v1.4.0 ■ POST.DS6_Risikenauszug.Kantone_
Result	Pass
Finding	N/A
Relevance	N/A

Table 22 – 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 <i>GetKey</i> algorithm) checks that the public key used to encrypt votes submitted by the persons voting corresponds to the

	<p>key that was created by the canton 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.</p> <p>The voting client application is composed of a HTML file (<i>index.htm</i>) and JavaScript files. The integrity of the JavaScript files can be checked by the voting persons thanks to the use of the <i>subresource integrity</i> 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 canton. The procedure is described in the Post's e-voting documentation.</p> <p>The e-voting documentation also provides instructions to verify the integrity of the <i>index.html</i> file manually.</p>
Evidence	<ul style="list-style-type: none"> ■ Swiss Post Voting System - System specification §5.1.3 ■ Instructions on how to verify the HTML and JavaScript files of the e-voting portal in the browser ■ E-voting demo website
Result	Pass
Finding	N/A
Relevance	N/A

Table 23 – Examination results: OEV paragraph 2.7.3

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

For soundness of the proofs referred to in Number 2.5

	2.9.1.2
	<p>The following system participants may be considered trustworthy:</p> <ul style="list-style-type: none"> ■ 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 24 – 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	<p>The following system participants may be considered trustworthy:</p> <ul style="list-style-type: none"> ■ 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 25 – 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: <ul style="list-style-type: none"> ■ 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 26 – Examination results: OEV paragraph 2.9.3.2

For the effectiveness of the authentication referred to in Number 2.8

Key	2.9.4.2
Requirement	The following system participants may be considered trustworthy: <ul style="list-style-type: none"> ■ set-up component ■ print component ■ 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.
Evidence	N/A
Result	N/A
Finding	N/A
Relevance	N/A

Table 27 – Examination results: OEV paragraph 2.9.4.2

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 28 – Examination results: OEV paragraph 2.1.3.3

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

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	<p>Components mentioned under Number 3.1 include:</p> <ul style="list-style-type: none"> ■ The set-up component, which operates in a controlled offline environment of the cantons and is used during the configuration phase. ■ At least one control component holding part of the decryption key, i.e., the <i>Tally Control Component</i>. This component derives the final decryption key from the electoral board members' passwords. It then performs the final decryption of the votes, factorises the decrypted data, decodes them into the corresponding voter selections, and tallies the results into the expected format. It runs in a controlled offline environment of the cantons. <p>The component mentioned under Number 3.3 is a technical aid: the <i>Verifier</i> software used by the auditors to check an election event. It also runs in a controlled offline environment of the cantons.</p> <p>Swiss Post operates four independent online control components. Each of these servers fulfils a dual role:</p> <ul style="list-style-type: none"> ■ as a <i>Return Codes Control Component (CCR)</i> during the voting phase, to generate and verify return codes; ■ as a <i>Mixing Control Component (CCM)</i> during the tallying phase, to shuffle the encrypted votes and perform partial decryption.
Evidence	<ul style="list-style-type: none"> ■ Infrastructure Whitepaper of the Swiss Post Voting System ■ Swiss Post Voting System - System specification §2,4, 2.6, 2,8, 2.9
Result	Pass
Finding	N/A

Relevance	N/A
-----------	-----

Table 29 – 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	<p>The CCR and CCM control components are the only trustworthy components under the sole responsibility of the Post.</p> <p>When performing changes to the control components, Swiss Post implements the notion of “observable process” by:</p> <ul style="list-style-type: none"> ■ Enforcing physical access control measures to limit the risks of unauthorised access; ■ Enforcing the four-eyes principle when accessing the control components (which involves persons from different teams); ■ Thoroughly documenting the accesses to the control components and related operations performed; ■ Forwarding access logs to its Security Information and Event Management (SIEM) system. <p>Logical access to the control components occurs via jumphosts, which log all actions performed and forward them to the Post’s SIEM. The teams interacting with the control components have no admin access to the jumphosts, nor access to the SIEM and are therefore not able to alter the session recording logs.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting – Zugriffskonzept Kontrollkomponenten (20/08/2025), §4.3, 5 ■ E-Voting – Change and Maintenance Concept (20/08/2025) ■ E-Voting – Security Elements Control Components (20/08/2025), §2.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 30 – Examination results: OEV paragraph 3.6

Key	3.7
Requirement	Before installing software, a published reference must be used for all programs to check whether the files are the correct and unaltered version.
Observation	<p>Swiss Post applies a trusted build and trusted deployment process to meet this requirement.</p> <p>The full source code of the Swiss Post e-voting system is permanently published on GitLab, along with the hashes of the trusted build artefacts, which constitute the official reference for comparison.</p> <p>Independent experts verify that the published source code corresponds to the software intended for execution and validate the list of published hashes as the trusted baseline.</p> <p>The <i>Trusted Deployment of the Swiss Post Voting System</i> document specifies that, during the software installation process, the hash values of the deployed artefacts are systematically checked against the published and validated reference hashes.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting - Release Management & Installation Concept (20/08/2025), §7.3 ■ Trusted Build and Trusted Deployment of the Swiss Post Voting System

	■ Trusted-Build
Result	Pass
Finding	N/A
Relevance	N/A

Table 31 – 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	<p>The e-voting system relies on public key cryptography to ensure the authenticity and integrity of configuration files, ballot definitions, results and reports through the use of digital signatures on exchanged data. In addition, confidentiality is guaranteed by encrypting ballots and verification codes with the election public key and other dedicated public keys generated by the control components.</p> <p>The exchange of the cryptographic material between Swiss Post and the canton bases on a direct trust model. In this model, the cryptographic keys and related material are exchanged directly and manually between the involved parties, without relying on an external public key infrastructure or intermediary certification authority. The cryptographic key stores and certificates distribution is performed using dedicated physical storage media (USB sticks with PIN protection).</p> <p>During the Direct Trust ceremony, USB sticks are dedicated to specific roles and are removed immediately after each upload step.</p> <p>The <i>Löschung der Daten</i> procedure requires that all removable media used during the voting process be deleted and reformatted after use, with the only exception of designated backup devices.</p>
Evidence	<ul style="list-style-type: none"> ■ Swiss Post Voting System - System specification, §7.1 ■ E-Voting - Schlüssel- und Zertifikatsmanagement Konzept (20/08/2025), §5 ■ E-Voting collaboration platform - Direct Trust Zeremonie - R1.4 (20/08/2025) ■ E-Voting collaboration platform - D4 - Löschung der Daten - R1.4 (20/08/2025), §2.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 32 – 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	<p>The updates of the e-voting system's components follow Swiss Post's corporate change and maintenance process, which is aligned with industry good practices as set out in ISO/IEC 27001 and based on a structured, risk-oriented approach.</p> <p>The e-voting specific <i>Change and Maintenance Concept</i> document defines distinct operational phases that determine when updates can be applied:</p> <ul style="list-style-type: none"> ■ Green phase (after a ballot, before preparation of the next one): updates to trustworthy components are performed, including installation of new releases,

	<p>patching of operating systems, runtimes and databases, renewal of certificates, and – if required – replacement of servers.</p> <ul style="list-style-type: none"> ■ Pre-red phase (system preparation before a ballot): no functional updates are applied to trustworthy components; activities focus on configuration checks, integrity verification and vulnerability scanning to confirm the readiness of the environment. ■ Red phase (voting preparation and active voting period): no updates of trustworthy components are permitted. Exceptions (e.g. urgent vulnerability fixes) require a formal risk assessment, multi-level approval, and supervised access to control components with canton participation. ■ Dark red phase (ballot counting weekend): a strict freeze applies; no updates of trustworthy components are allowed. <p>Through this phased approach, updates to trustworthy components are scheduled in a way that ensures the expected benefits outweigh the potential risks</p>
Evidence	<ul style="list-style-type: none"> ■ Change Management – Richtlinie (20/08/2025) ■ Change and Maintenance Concept - E-Voting (20/08/2025), §4 ■ E-Voting - Release Management & Installation Concept (20/08/2025), §8
Result	Pass
Finding	N/A
Relevance	N/A

Table 33 – Examination results: OEV paragraph 3.9

Key	3.11
Requirement	Trustworthy components may not be connected to the internet when installing or updating software.
Observation	<p>As a default rule, the Post's servers located in internal zones, such as the control components (i.e., the trustworthy components under the sole responsibility of the Post), are not allowed to communicate with external services (i.e., on Internet). No exception is in place for the control components.</p> <p>No update is performed on control components. They are always reinstalled from scratch, and the process is performed offline.</p>
Evidence	<ul style="list-style-type: none"> ■ Infrastructure Whitepaper of the Swiss Post Voting System ■ IT20 Workspace – NB Network Security Architecture (20/08/2025), §7.7.2 ■ E-Voting - Release Management & Installation Concept (20/08/2025), §7.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 34 – 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	Swiss Post's <i>Konzept zur Datenvernichtung</i> document mentions that all data related to a voting event be deleted after the completion of the ballot. The deletion is initiated upon a formal request by the responsible canton and carried out as an internal IT change. For control components, data is erased during the maintenance window following each ballot, either by reinstalling the systems or by applying the secure deletion methods of the operating system. Where justified reasons exist, such as ongoing legal appeals, data may be retained under secure storage conditions before destruction.
Evidence	Konzept zur Datenvernichtung – E-Voting (20/08/2025)
Result	Pass
Finding	N/A
Relevance	N/A

Table 35 – Examination results: OEV paragraph 3.12

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	<p>Logical access to the control components (i.e., the trustworthy components under the sole responsibility of the Post) is designed in a way that enforces the four-eyes principle (operations are performed in presence of two persons from two different teams) and segregation of duties.</p> <p>Access to the control components by system or database administrators is performed by submitting an access request to the Operations Control Center (“OCC”) team, which itself has no access to the network zones where the control components reside. Access to the Linux-based control components is allowed through the allocation of a token (under the form of a one-time authentication token) to the requestor, and to the temporary integration to an Active Directory group for the Windows-based control component, once the token team has verified the identity of the requestor and validated the need for access (it verifies the existence of a service or incident ticket, or change request). All logical actions on control components are subject to a formal report signed by the parties involved.</p> <p>Logical access to the control components occurs via jumphosts, which log all actions performed (logs are forwarded to the Post's Splunk Security Information and Event Management (SIEM) system). The control components' administrators have no admin access to the jumphosts.</p> <p>Out-of-Band Management tools (HP's iLO and Cisco's CIMC) are available. Access permissions to these management interfaces are granted following the same authorisation process as depicted above.</p> <p>Teams with logical access to the control components do not have physical access and vice versa. Only the <i>Datacenter & Connectivity</i> team is permitted to access the components physically, based on a formal change request. All physical actions on control components are subject to a formal report signed by the parties involved.</p> <p>During their on-site visit to one of the data centres hosting the control components (on September 17th), the examiners observed that the four-eyes principle had not been applied during the last physical interventions on the control components, as only one name appeared in the corresponding logs. Swiss Post initiated a corrective action plan to address this issue. The new procedure, effective since October 7th, now requires all physical interventions to be performed under supervision: personnel physically accessing the control components do not know the codes to the safes where the keys to the equipment racks are stored and are therefore unable to gain access</p>

	<p>unaccompanied.</p> <p>The Post's employees are not involved in the management of data carriers processing e-voting data, which is the responsibility of the cantons.</p> <p>However, USB sticks are used to install on the control components their keystores, as well as the certificates of the trustworthy components operated by the cantons. Once the cryptographic material has been successfully installed, the USB sticks are securely deleted. The deletion process is carried out under the four-eyes principle and is fully logged.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting - Benutzeranleitungen Release 1.5 (20/08/2025) ■ E-Voting – Zugriffskonzept Kontrollkomponenten (20/08/2025), §4.3, ■ E-Voting - Physical Access Data Center E-Voting Infrastructure concept v26 ■ Concept de remédiation à la non-conformité d'accès aux composants de contrôle (30/09/2025) ■ Infrastructure Whitepaper of the Swiss Post Voting System ■ E-Voting collaboration platform - Direct Trust Zeremonie - R1.5 (28/10/2025), §6
Result	Pass
Finding	N/A
Relevance	N/A

Table 36 – Examination results: OEV paragraph 3.14

Key	3.15
Requirement	<p>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:</p> <ul style="list-style-type: none"> ■ 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	<p>Logical access to the control components is performed by two teams acting at different layers :</p> <ul style="list-style-type: none"> ■ The OS team installs and manages the operating systems in accordance with security best practices; ■ The control component team installs and configures the applications and services required for the secure operation of the e-voting system. <p>Separate dedicated teams (i.e., CC1, CC2, CC3, CC4) are responsible of each of the four control components operated by Swiss Post, enforcing proper segregation of duties.</p> <p>Each control component runs on dedicated physical hardware with distinct operating system (i.e., RedHat, Debian, Ubuntu, Windows) and is operated in a dedicated network. However, three out of the four control components run on similar server type (<i>ProLiant BL460c Gen10</i>). While the present requirement recommends maximum diversity of hardware, operating systems, and monitoring systems across the control components, Swiss Post applies a standardised hardware approach for operational efficiency and maintainability. Three of the four control components therefore operate on servers of the same model, with two distinct hardware types overall.</p>

	<p>Similarly, the use of a separate monitoring systems for each control component would introduce significant operational complexity and contradict the principle of centralised log management. Swiss Post has therefore chosen a centralised monitoring architecture while maintaining strict logical segregation of logs for each control component.</p> <p>Access to the control components' networks is disabled by default and must be explicitly granted, based on a formal access request. Logical access to a given control component occurs through a dedicated jump host. Therefore, compromising one jump host would not procure any advantage in an attempt to access another control component.</p> <p>From a physical perspective, each control component operates in a dedicated rack located in the most secure zone of the datacentre provider (PostFinance). Physical access is restricted to the <i>Datacenter & Connectivity</i> team, which is responsible for hardware installation. However, during their on-site visit (on September 17th), the examiners observed a gap in terms of segregation of duties within the team: all six members had access to all four control components. Swiss Post initiated a corrective action plan to address this issue. The keys to the racks hosting the control components are now stored separately in dedicated safes. The next step of the plan involves hosting the control components in its own rack with a distinct key lock. This phase is scheduled for December 2025. The examiners consider that this planned setup will fulfil the present requirement regarding segregation of duties.</p>
Evidence	<ul style="list-style-type: none"> ■ Infrastructure Whitepaper of the Swiss Post Voting System ■ E-Voting – Security Elements Control Components (20/08/2025), §2.1 ■ E-Voting – Zugriffskonzept Kontrollkomponenten (20/08/2025), §4.1, 5 ■ E-Voting – Organizational concept (20/08/2025), §6.2 ■ Technical Specifications of the Main Components of the E-Voting System ■ Concept de remédiation à la non-conformité d'accès aux composants de contrôle (30/09/2025)
Result	Pass
Finding	N/A
Relevance	N/A

Table 37 – 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	<p>Any logical access performed on a control component is monitored, recorded and corresponding alerts are sent to the E-Voting team.</p> <p>Resistance to manipulation of logs during their transfer is provided thanks to the use of TLS with mutual authentication between the e-voting system and the monitoring tools.</p> <p>The rooms where the control components are hosted are subject to physical access control and video surveillance.</p> <p>The Post applies the following measures to ensure the trustworthiness of its employees:</p> <ul style="list-style-type: none"> ■ Performance of background checks (as part of the general Post HR process, a criminal record extract is required for joiners and movers and additional elements may be required by the team leaders such as a certificate from the debt

	enforcement office); <ul style="list-style-type: none"> ■ Signature by the personnel of non-disclosure agreement (as part of the general Post HR process and e-voting-specific).
Evidence	<ul style="list-style-type: none"> ■ Infrastructure Whitepaper of the Swiss Post Voting System ■ E-Voting – Zugriffskonzept Kontrollkomponenten (20/08/2025), §4.2, 4.3, 5.4, 6 ■ E-Voting – Organizational concept (20/08/2025), §6.1.1, 6.1.2 ■ Manuel – Contrôle de sécurité du personnel V02.00 ■ E-Voting – Monitoring concept (20/08/2025), §3.1, 4.1, 4.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 38 – Examination results: OEV paragraph 3.16

Key	3.17
Requirement	Trustworthy components may perform only the intended operations
Observation	<p>The trustworthy components operated by Swiss Post are the four independent online control components. Each of these servers fulfils a dual role:</p> <ul style="list-style-type: none"> ■ as a <i>Return Codes Control Component (CCR)</i> during the voting phase, to generate and verify return codes; ■ as a <i>Mixing Control Component (CCM)</i> during the tallying phase, to shuffle the encrypted votes and perform partial decryption. <p>The following measures provide assurance that those components perform only the intended operations:</p> <ul style="list-style-type: none"> ■ The <i>Trusted Build and Deployment</i> process guarantees that only artifacts derived from the published source code are installed, with hash verification mitigating the risk of unauthorized functionality; ■ The control components are subject to hardening measures, including minimal service configuration, strict access control, and separation-of-duties for administrative actions, thereby limiting the risk of unintended use; ■ Continuous monitoring and audit logging are implemented to detect anomalous behaviour or operations outside the defined scope; ■ Functional and security testing systematically validate that control components operate in accordance with their defined specifications, reducing the risk of unnoticed deviations.
Evidence	<ul style="list-style-type: none"> ■ Swiss Post Voting System - System specification, §2,4 ■ E-Voting – Security Elements Control Components (20/08/2025)
Result	Pass
Finding	N/A
Relevance	N/A

Table 39 – Examination results: OEV paragraph 3.17

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	<p>Quality and document management within the e-voting organization follow a structured approach. A document management system ensures version control, ownership, classification, and periodic reviews, while enforcing naming conventions and standardized structures. Processes related to e-voting infrastructure and operation are formally modelled in the corporate process management tool where necessary, ensuring that workflows are documented in a consistent and transparent manner. This contributes to the clarity of all procedures.</p> <p>All documentation related to the e-voting system is available on the Post's e-voting internal wiki. To ensure completeness, accuracy and readability of the documentation, each wiki page is assigned an owner, in charge of its maintenance.</p> <p>The <i>Release Management & Installation Concept</i> document refers to the following documents:</p> <ul style="list-style-type: none"> ■ Installation checklist and report for control component servers; ■ Installation protocol and report control component operating systems; ■ Trusted Build and deployment process (installation of the e-voting release following an installation checklist) <p>Swiss Post also applies a formal change management process, ensuring that any modification to the production environment is formally recorded as a change and documented.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting – Release Management & Installation Concept (20/08/2025), §7 ■ E-Voting – Change and Maintenance Concept (20/08/2025), §4.1 ■ E-Voting – Organizational Concept (20/08/2025), §5.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 40 – 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	<p>Every access and action performed on a control component is subject to a formal access request and report. Logical access is only possible via a jump host. All interactive sessions initiated from the jumphosts are recorded.</p> <p>Hardening measures applied on the control components include the activation of local logging functionalities.</p> <p>Logical accesses performed on control components trigger an alarm which is sent to the e-voting DevOps team, in charge of monitoring.</p> <p>After each ballot, local access logs are reconciled with the records of the team granting accesses (OCC) to ensure consistency.</p> <p>The deletion actions performed on the USB sticks used during the Direct Trust ceremony between Swiss Post and the cantons are likewise logged.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting – Zugriffskonzept Kontrollkomponenten (20/08/2025), §4.3, 5 ■ E-Voting – Monitoring concept (20/08/2025), §4.1, 4.2 ■ E-Voting – Security Elements Control Components (20/08/2025), §2.8 ■ E-Voting collaboration platform - Direct Trust Zeremonie - R1.5 (28/10/2025), §6
Result	Pass
Finding	N/A

Relevance	The concept of “trusted component” is not defined in the OEV, which prevents an objective interpretation of the examination criterion. The examiners assimilated it to the term of “trustworthy component”.
------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Table 41 – Examination results: OEV paragraph 3.20

Information and instructions

Key	8.13
Requirement	Known flaws and the need for action associated with them are communicated transparently
Observation	Swiss Post maintains a section related to known issues on its public GitLab instance.
Evidence	https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/issues
Result	Pass
Finding	N/A
Relevance	N/A

Table 42 – Examination results: OEV paragraph 8.13

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 final decryption of votes and the tallying process are performed exclusively within the canton’s controlled environment, using the Tally Control Component. The secret key required for the final decryption is derived from the passwords of the electoral board members, which are only available to them. Swiss Post has no access to this component or to the keys involved in the decryption. As a result, the timing of the decryption is solely determined by the canton, with no means for Swiss Post to influence it.
Evidence	Swiss Post Voting System - System specification § 2,8
Result	Pass
Finding	N/A
Relevance	N/A

Table 43 – Examination results: OEV paragraph 11.1

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	Swiss Post is not involved in either the decryption process or the transmission of the ballot results, which are fully performed under the responsibility of the cantons. Access to the e-voting application and infrastructure by Swiss Post is governed by the organization’s e-voting-specific change management process. During the <i>Dunkelrote</i>

	<p><i>Phase</i> (the critical period from Saturday to Sunday of the ballot weekend), a strict change freeze applies: no modifications to the e-voting systems or related infrastructure are permitted.</p> <p>In exceptional cases requiring access to the e-voting components, the process mandates:</p> <ul style="list-style-type: none"> ■ Access to be carried out in a monitored remote session involving representatives of the affected cantons, the Operations Control Center (OCC), and the Swiss Post e-voting team; ■ Full documentation of every step to ensure complete traceability and auditability; ■ A mandatory root cause analysis and incident report following any intervention.
Evidence	E-Voting – Change and Maintenance Concept, §4.6
Result	Pass
Finding	N/A
Relevance	N/A

Table 44 – Examination results: OEV paragraph 11.4

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	<p>One of the core security objectives of the Swiss Post e-voting system is to ensure vote secrecy, i.e., to prevent any party from learning information about the cast votes beyond what is inevitably revealed by the election result. This property is achieved by the cryptographic protocol, which ensures that votes are always encrypted before reaching any component operated by Swiss Post and remain encrypted throughout their processing. The correctness of the protocol and its cryptographic implementation are outside the scope of this audit and are subject to dedicated cryptographic assessments.</p> <p>From an infrastructure and operations perspective, Swiss Post implements several controls to reduce the risk of unauthorized access to vote data or the insertion of malicious code within the environment it operates, e.g.,</p> <ul style="list-style-type: none"> ■ End-to-end encryption (TLS 1.3) to protect communications between the voter’s browser and the Swiss Post voting servers, ensuring the confidentiality and integrity of data transmitted and allowing voters to authenticate the voting server; ■ Client-side code verification mechanisms allow external parties and researchers to verify that the JavaScript and HTML executed in voters’ browsers match the published reference source code, enabling detection of any unauthorized modifications aimed at capturing voter choices before encryption; ■ Hardening and segmentation of servers and networks, applying the principle of least privilege to minimize attack surfaces; ■ Background checks and role-based access control, ensuring that only vetted and trusted personnel have access to sensitive systems; ■ Controlled and supervised access to critical systems, enforced through the four-eyes principle and tamper-resistant logging; ■ Trusted Build and Trusted Deployment processes to confirm that only artifacts derived from the reviewed and published source code are deployed to production systems, ■ Continuous security testing, including public source code review, a bug bounty program, and regular penetration tests, to detect vulnerabilities such as malicious

	script injection or unauthorized code execution; <ul style="list-style-type: none"> ■ Etc.
Evidence	<ul style="list-style-type: none"> ■ Protocol of the Swiss Post Voting System v1.4.0, §2.4 ■ Infrastructure Whitepaper of the Swiss Post Voting System
Result	Pass
Finding	N/A
Relevance	N/A

Table 45 – 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 premature results to be determined.
Observation	<p>As mentioned in the audit observation for Number 12.1, one of the core security objectives of the Swiss Post e-voting system is vote secrecy. By extension, vote secrecy ensures that no component can determine partial or final election results before the official decryption step. According to the system specification, this property is achieved by encrypting votes end-to-end and splitting the decryption key among multiple independent entities, so that no single party, including Swiss Post, can decrypt votes on its own.</p> <p>As a result, Swiss Post only ever processes encrypted votes. The decryption keys required to obtain plain-text votes are never present in Swiss Post’s infrastructure and remain entirely under the control of the canton. The correctness of this cryptographic mechanism and the security of the decryption process itself are outside the scope of this audit and are covered by dedicated assessments.</p> <p>The infrastructure and operational measures described in the observation for Number 12.1 also reduce the risk of premature determination of results.</p>
Evidence	<ul style="list-style-type: none"> ■ Swiss Post Voting System - System specification, §1.2 ■ Infrastructure Whitepaper of the Swiss Post Voting System
Result	Pass
Finding	N/A
Relevance	N/A

Table 46 – Examination results: OEV paragraph 12.2

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	<p>Swiss Post maintains a documented process concerning the destruction of all electronic data created as part of a ballot, i.e.,</p> <ul style="list-style-type: none"> ■ Votes cast (stored in encrypted form within the control components and e-voting server databases, with the decryption key exclusively held by the cantons); ■ Reverse proxies logs (stored in encrypted form); ■ E-voting application server logs; ■ Control component logs; ■ Firewall logs;

	<ul style="list-style-type: none"> ■ Database logs; ■ Security Information and Event Management (SIEM) system logs, including logs generated by the reverse proxies, application servers and control components; ■ Backup data (note: SIEM and databases logs are not included in backups). <p>The destruction of this data takes place upon instructions from the cantons, once the legal appeal period within the election process has expired and any valid appeals have been fully processed.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting – Konzept zur Datenvernichtung (20/08/2025) ■ E-Voting - Benutzeranleitungen Release 1.5 (20/08/2025), §8
Result	Pass
Finding	N/A
Relevance	N/A

Table 47 – 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	<p>All threats listed in Numbers 13.3-13.40 are considered by Swiss Post in its risk assessment related to the e-voting system. Additional custom threats relevant to the e-voting context have been added to the list:</p> <ul style="list-style-type: none"> ■ Attack by quantum computer against vote secrecy; ■ Sabotage of the infrastructure by an internal attacker; ■ Information leakage within the infrastructure by an internal attacker. <p>Risks are evaluated according to Swiss Post's general information security risk management process, which is based on the Credible Worst Scenario method and uses a 6x6 scoring model. Each risk is documented with a description of the main mitigation measures implemented and mapped to the corresponding ISO/IEC 27002 security controls. Risks are reviewed on a yearly basis.</p>
Evidence	<ul style="list-style-type: none"> ■ POST.DS6_Risikenauszug.Kantone_ ■ Handbuch Risikomanagement DS v04.01
Result	Pass
Finding	N/A
Relevance	N/A

Table 48 – Examination results: OEV paragraph 13.1

Key	13.2 – 13.40
Requirement	<p>The following are considered to be potential threats:</p> <ul style="list-style-type: none"> ■ Inadvertent or intended electronic or physical threats from internal or external actors; ■ Threats resulting from a malfunction of the system or system-supporting elements.

Observation	The listed threats have been considered in the Information Security and Data Privacy concept and risk register elaborated by Swiss Post regarding the e-voting system.
Evidence	<ul style="list-style-type: none"> ■ POST.DS6_Risikenauszug.Kantone_ ■ ISDS Konzept (ISDS DS E-Voting (SDOC-3200417))
Result	Pass
Finding	N/A
Relevance	N/A

Table 49 – 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	<p>An infrastructure monitoring system detects incidents that could endanger the security, including availability, of the system and alerts the responsible personnel. The personnel deal with incidents according to a predetermined procedure. Crisis scenarios and rescue plans serve as guidelines (and include a plan that guarantees that voting-related activities can continue) and are applied as required.</p> <p>Errors in the registration of votes in the control components and in the ballot box must be detected. Further information relating to the error must be available in order to identify and eliminate the cause. Any incidents detected must be reported to the body responsible at cantonal level.</p>
Observation	<p>Incident and anomaly logs related to the e-voting system infrastructure are collected within Swiss Post's general Security Information and Event Management (SIEM) system. Alerts are handled by a 24/7 on-call duty team in accordance with the e-voting-specific incident management process.</p> <p>Errors in vote registration are detected at the application layer of both the voting servers and the control components, as well as through telemetry at the Artemis message broker level, where queues fill up in case of an issue.</p> <p>A set of predefined incident scenarios has been established to ensure efficient handling in case of occurrence, including appropriate coordination with the cantonal authorities.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting – Monitoring Concept (20/08/2025), §4.1, 4.2, 5 ■ E-Voting – Emergency Concept (20/08/2025), §5 ■ E-Voting - E-Voting Incident Management Concept (EVIMC) (20/08/2025)
Result	Pass
Finding	N/A
Relevance	N/A

Table 50 – Examination results: OEV paragraph 14.1

Key	14.2
Requirement	<p>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.</p>

	<p>The content of the records covers at least the following events:</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>The system logs are made available to the body responsible at cantonal level in such a way that it can interpret the information.</p>
Observation	<p>All IT components supporting the e-voting system (e.g., network components, servers, the Kubernetes container orchestration system, the Artemis message broker, middleware, e-voting software, databases, etc.) generate extensive logs that are formatted and forwarded to Swiss Post's security information and event management (SIEM) system. The transmission occurs over TLS, and they cannot be edited in the SIEM, which guarantees their integrity.</p> <p>Logs are time-stamped using a common NTP source and time zone to ensure consistency.</p> <p>The e-voting system is built in accordance with the 12 <i>Factor App principles</i>, including log management, which requires applications to write all log events to standard output so that the execution environment can collect and route them to the SIEM. The precise nature of the events to be logged in relation to a ballot is defined at the application level, which is not part of the present evaluation scope.</p> <p>Collected logs include events related to malfunctions at infrastructure level.</p> <p>Daily consolidated reports about received alerts are generated and transmitted to the cantons. These reports include:</p> <ul style="list-style-type: none"> ■ A summary of incidents and alerts; ■ Investigative insights into anomalies; ■ Statistical data for trend analysis and performance evaluation.
Evidence	<ul style="list-style-type: none"> ■ E-Voting – Monitoring Concept (20/08/2025), §3.1, 6.2, 7.1 ■ IT20 Workspace - HB Network Security Architecture (HNSA) (20/08/2025) - §7.1.4 ■ Swiss Post Voting System v1.5.0 – Software Architecture Document, §8.1.1 ■ E-Voting collaboration platform- Debriefing – UG – 2025-02-09
Result	Pass
Finding	N/A
Relevance	N/A

Table 51 – 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	Swiss Post applies a structured continuous improvement process for monitoring and logging. After each incident, a formal debriefing is conducted with all relevant stakeholders to review the timeline, determine the root cause, and identify gaps in logging and alerting processes. Identified issues and proposed improvements are documented, tracked, and monitored until resolution. Logging practices are periodically reviewed to ensure critical

Evidence	<p>events are captured, log formats are consistent, and redundant logs are removed.</p> <ul style="list-style-type: none"> ■ E-Voting – Monitoring Concept (20/08/2025), §7 ■ E-Voting collaboration platform- Debriefing – UG – 2025-02-09
Result	Pass
Finding	N/A
Relevance	N/A

Table 52 – 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 ensure voting secrecy
Observation	<p>From a design perspective, the Swiss Post voting system enforces strict separation between vote data and monitoring data: No data related to votes is stored in plaintext or logged within Swiss Post’s infrastructure.</p> <p>End-to-end encryption guarantees that all votes are encrypted on the voter’s device and only decrypted offline on cantonal premises during tallying. Therefore, components operated by Swiss Post only process encrypted data and cannot access vote contents or determine premature results.</p> <p>With respect to logs and metrics:</p> <ul style="list-style-type: none"> ■ Reverse proxy logs contain only operationally essential fields (e.g., client IP address, user-agent) required for diagnostic and security purposes; ■ Application logs and metrics are designed and developed according to predefined coding guidelines to capture only operationally relevant, non-sensitive data. Sensitive elements, such as vote choices or authentication credentials, are strictly excluded, with anonymization or masking applied where needed.
Evidence	<ul style="list-style-type: none"> ■ E-Voting – Monitoring Concept (20/08/2025), §3.1, 3.2 ■ Security Whitepaper of the Swiss Post Voting System
Result	Pass
Finding	N/A
Relevance	N/A

Table 53 – Examination results: OEV paragraph 14.4

Key	14.5
Requirement	It must be guaranteed that in the event of a malfunction, the votes and the data that prove the smooth operation of the vote tallying are stored safely in the infrastructure.
Observation	<p>The e-voting system’s infrastructure is deployed with redundancy (triple active mode, two geographically distinct datacentres) to maintain operations in case of individual component failure. Critical services are distributed across multiple instances with load balancing and dynamic scaling to handle peak loads and maintain continuous availability. Control components are also deployed on multiple nodes in separate environments, supporting fault tolerance and reducing the risk of service interruption.</p> <p>All critical data related to the voting process is backed up in encrypted form.</p>
Evidence	<ul style="list-style-type: none"> ■ Infrastructure Whitepaper of the Swiss Post Voting System ■ Swiss Post Voting System architecture document §10.5.2 ■ E-Voting - Data Backup Concept (20/08/2025), §2.2 – 2.6

Result	■ E-Voting – Emergency Concept (20/08/2025), §5.1.2, 5.2.2, 5.2.3, 5.3.3
	Pass
	Finding
	N/A
Relevance	N/A

Table 54 – Examination results: OEV paragraph 14.5

Key	14.6
Requirement	After a breakdown in the system or a failure of communication or storage media, the system enters a recovery mode in which it is possible to return to a safe state. Voting processes that have been started are interrupted. The person voting cannot resume voting until the system is returned to a secure state.
Observation	<p>The e-voting system implements strong technical resilience measures to ensure system availability in case of component or site failure.</p> <p>Failover mechanisms are tested regularly as part of the Disaster Recovery concept, with automatic recovery expected within one hour and manual recovery procedures in place for major incidents. Voting data, such as encrypted ballots and voting card states, is securely persisted in high-availability databases and backed up to prevent data loss.</p> <p>The system is engineered to recover from component crashes, network interruptions, or storage/media failures and to return to a safe operating state before processing continues. The following architecture principles have been integrated into the design:</p> <ul style="list-style-type: none"> ■ Stateless, disposable runtime services with persisted critical state: Most runtime services are stateless and disposable (Kubernetes can stop/restart instances cleanly), while critical state is persisted in durable stores (e.g., PostgreSQL for Voting Server/Control Components; filesystem/SQLite for SDM); ■ Reliability and fault tolerance: <ul style="list-style-type: none"> ● Automatic reconnection/retry with timeouts for broker/DB connections ● Failure compartmentalization; ● Instances rejoin service only once healthy; ● Elastic recovery on Kubernetes; ■ Durable persistence and recovery points: Voter-related records and control-component state are durably stored in highly available databases; SDM work is persisted locally (and via offline media for air-gapped SDM), providing recovery points after failures; ■ Transactional messaging and idempotent processing: Message consumption is transactional and operations are idempotent/exactly-once using ACID transactions; in-flight processes are rolled back on errors and only resume once consistency is re-established; ■ Database high availability with controlled failover: Synchronous replication prevents acknowledged data loss; failover is performed manually to avoid split-brain, prioritizing integrity and ensuring a verified safe state before resuming; <p>Any voting process that was in progress at the time of failure is interrupted by the above mechanisms and cannot continue until the system has recovered to a verified secure state.</p>
Evidence	<ul style="list-style-type: none"> ■ Infrastructure Whitepaper of the Swiss Post Voting System ■ E-Voting – Emergency Concept (20/08/2025), §5.2.3 ■ E-Voting - Disaster Recovery concept (20/08/2025), ■ E-Voting - E-Voting Incident Management Concept (EVIMC) ■ Swiss Post Voting System architecture document, §5.4, 8.1.1, 9.1.9, 10.1.2, 10.5.2

Result	Pass
Finding	N/A
Relevance	N/A

Table 55 – Examination results: OEV paragraph 14.6

Key	14.8
Requirement	Infrastructure availability must be checked and recorded at selected intervals.
Observation	The e-voting system includes continuous monitoring of infrastructure availability through health checks, metrics, and centralised dashboards. During a ballot, automated alerts notify operations teams of failures or degraded performance, and incidents are managed through a structured process with reporting to cantonal authorities.
Evidence	E-Voting – Monitoring Concept (20/08/2025), §4.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 56 – 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	Swiss Post has a defined process for managing known vulnerabilities (<i>Vulnerability Treatment – Schwachstellenanalyse durchführen</i>). E-voting system components are updated following Swiss Post’s general change management process, which is aligned with best practices. In addition, a specific change and maintenance management concept defines how updates for the e-voting components are planned and executed: Updates are carried out during the <i>Green Phase</i> , a maintenance period when no elections are in progress, covering tasks such as security patching, new releases, system updates, and certificate renewals. During the <i>Red Phase</i> , from the setup to the closing of a ballot, changes are avoided to reduce technical risks. Only essential updates, such as landing page changes or urgent security fixes, are allowed and must be approved through a defined process with systematic involvement of cantonal authorities and the Federal Chancellery.
Evidence	<ul style="list-style-type: none"> ■ Vulnerability Treatm. – Schwachstellenanalyse durchführen V01.08 ■ Change Management – Change Management Richtlinie – (20/08/2025) ■ E-Voting – Change and Maintenance Concept (20/08/2025), §4
Result	Pass
Finding	N/A
Relevance	N/A

Table 57 – 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	The <i>E-Voting – Monitoring Concept</i> document describes the types of logs collected for the e-voting components, including system usage, administrator logins and activities, and system malfunctions. It also contains a section on the continuous improvement of logging practices, which covers debriefing meetings after unexpected incidents, tracking identified issues, and implementing recommendations to improve log coverage, format, and efficiency.
Evidence	E-Voting – Monitoring Concept (20/08/2025)
Result	Pass
Finding	N/A
Relevance	N/A

Table 58 – 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	<p>The management of certificates within Swiss Post is governed by a corporate cryptographic security policy based on industry best practices. This policy defines requirements for:</p> <ul style="list-style-type: none"> ■ The management of cryptographic material throughout its lifecycle; ■ The selection of algorithms according to specific use cases; ■ The approved cryptographic protocols and associated algorithms; ■ The generation of random numbers. <p>It also defines the roles and responsibilities of stakeholders to ensure proper management of cryptographic material.</p> <p>At the e-voting level, Swiss Post has issued a dedicated concept for managing cryptographic keys and certificates (excluding the keys used exclusively within the e-voting cryptographic protocol, which are outside the scope of this audit). Certificate use cases include:</p> <ul style="list-style-type: none"> ■ Implementing the TLS protocol on both public-facing and internal servers, between Rancher Kubernetes Engine components, and on clients for mutual authentication; ■ Digitally signing and encrypting messages exchanged between Swiss Post and the cantons during e-voting operations.
Evidence	<ul style="list-style-type: none"> ■ Architecture & Technology – HB Kryptographie (20/08/2025), §3.2.4 ■ E-Voting - Schlüssel- und Zertifikatsmanagement Konzept (20/08/2025) ■ E-Voting – Zugriffskonzept Kontrollkomponenten (20/08/2025) ■ Swiss Post Voting System - System specification, §7
Result	Pass
Finding	N/A
Relevance	N/A

Table 59 – 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	<p>According to the OEV definition, <i>Critical data</i> are data whose integrity or confidentiality is decisive in meeting the cryptographic protocol requirements.</p> <p>The Swiss Post e-voting system employs cryptographic measures aligned with state-of-the-art practices to protect the integrity and confidentiality of critical data including identification and authentication data of the authorities (i.e., the cantons). Transport Layer Security (TLS) is used to protect communications between clients (voters and cantonal systems) and the Swiss Post Access Layer. TLS certificates for online components are issued by trusted certificate authorities and rotated annually. Mutual authentication is enforced for communications between cantonal systems and Swiss Post.</p> <p>In addition to transport layer protections, the e-voting system enforces application-layer channel security through the Secure Data Manager (SDM). This component applies cryptographic measures to ensure that only authorized entities can exchange and interpret sensitive data. Specifically, the SDM uses:</p> <ul style="list-style-type: none"> ■ Authenticated encryption with AES-GCM-256 to provide confidentiality and integrity of messages and files; ■ Digital signatures using RSASSA-PSS with 3072-bit RSA keys and SHA-256 to guarantee authenticity and integrity. <p>These protections are applied to structured messages exchanged between cantonal infrastructure and control components operated by Swiss Post.</p> <p>Furthermore, backups of critical data related to vote tallying are protected with end-to-end encryption, ensuring its security both in transit and at rest:</p> <ul style="list-style-type: none"> ■ Data in transit is encrypted using SSH or TLS 1.3; ■ Data at rest is encrypted using AES-256. <p>The management of cryptographic keys is defined within the <i>HB Kryptographie</i> document and follows best practices, covering the entire lifecycle of cryptographic material.</p> <p>Swiss Post conducts threat modelling as part of the e-voting system's architectural design to systematically identify the security measures – including cryptographic controls – needed to protect critical data processed by the system.</p>
Evidence	<ul style="list-style-type: none"> ■ Infrastructure Whitepaper of the Swiss Post Voting System ■ Swiss Post Voting System - System specification ,§7 ■ Crypto primitives specification, §6, 7 ■ E-Voting Data Backup Concept (20/08/2025), §2.9 ■ Architecture & Technology – HB Kryptographie (20/08/2025), §3.2.3 ■ E-Voting – Schlüssel- und Zertifikatsmanagement Konzept (20/08/2025) ■ E-Voting – Threat modeling (20/08/2025)
Result	Pass
Finding	N/A
Relevance	N/A

Table 60 – 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	As outlined in Number 15.2, cryptographic measures are widely used in the e-voting infrastructure to protect critical data in transit and at rest following best practices defined within the <i>HB Kryptographie</i> document.
Evidence	<ul style="list-style-type: none"> ■ Infrastructure Whitepaper of the Swiss Post Voting System ■ Swiss Post Voting System - System specification ,§7 ■ Crypto primitives specification, §6, 7 ■ E-Voting Data Backup Concept (20/08/2025), §2.9 ■ Architecture & Technology – HB Kryptographie (20/08/2025), §3.2.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 61 – 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 ⁶ on Electronic Signatures (ESigA). The signature must be verified by means of a certificate that has been issued by a recognised supplier of certificate services under the ESigA.
Observation	Key lengths and algorithms used within the e-voting cryptographic components correspond to current standards, According to tables 15, 16 and 17 of the <i>System specification</i> document, there are 28 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.
Evidence	<ul style="list-style-type: none"> ■ Swiss Post - Cryptographic Primitives of the Swiss Post Voting System – Pseudocode Specification, §2 ■ Swiss Post Voting System - System specification, §7.1 ■ Architecture & Technology – HB Kryptographie (20/08/2025), §3
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 62 – Examination results: OEV paragraph 15.4

⁶ SR 943.03

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	<p>The access layer to the e-voting system is composed of:</p> <ul style="list-style-type: none"> ■ Load balancers which are common to the whole Swiss Post infrastructure; ■ Dedicated virtual Apache reverse proxies by canton (one for administration access, one for voter access), running on redundant blade servers, which are located in dedicated DMZ (i.e., the Access zone). <p>The e-voting server components implement a microservice architecture made of containers, whose lifecycle is controlled by the Kubernetes container orchestration platform. Each canton has its own e-voting instance, defined as a Rancher project with its own Kubernetes namespace. Firewall rules ensure the appropriate isolation of each Rancher project. Each worker node is a virtualised machine based on the VMWare technology. Communications between the various Kubernetes pods and nodes supporting the e-voting systems are filtered at OSI layer 4 level (port) using Kubernetes network policies.</p> <p>The control components are hosted in dedicated zones within the Post's internal network, that represent trust boundaries between the individual components. Ingress and egress traffic is firewalled.</p> <p>The implementation of the e-voting components appears to satisfy the requirements of the Post's Network Security Architecture policy. The policy defines trust zones and the communication rules between the said zones. It requires to filter communications through firewalls at OSI layer 4 level between some zones and forbids communications from specific zones to others (e.g., from the Admin zone to Internet).</p>
Evidence	<ul style="list-style-type: none"> ■ Infrastructure Whitepaper of the Swiss Post Voting System ■ IT20 Workspace – NB Network Security Architecture (20/08/2025),
Result	Pass
Finding	N/A
Relevance	N/A

Table 63 – Examination results: OEV paragraph 16.1

Key	16.2
Requirement	The systems must be protected against attack (irrespective of the nature of the attack or of its origin).
Observation	<p>From an infrastructure and operations perspective, Swiss Post applies a broad range of security assurance measures to protect the e-voting system against internal and external attacks. The <i>Security Whitepaper of the Swiss Post Voting System</i> document describes the following practices:</p> <ul style="list-style-type: none"> ■ Threat modelling: <ul style="list-style-type: none"> ● Application of STRIDE methodology, extended with e-voting-specific risks (e.g., accuracy of results, secrecy of votes, availability of the system, and protection of voter-related information); ● Integration of the Federal Chancellery's mandated risk categories and the general threat catalogue (Ordinance, §13.3–13.40) into risk assessments; ■ Layered security controls: Security relies on multiple, complementary layers

	<p>combining preventive, detective and corrective controls at both the technical and organisational levels.</p> <ul style="list-style-type: none"> ■ Secure software development and deployment: <ul style="list-style-type: none"> ● Use of a trusted build pipeline and controlled release management, ensuring that the code deployed in production corresponds to the reviewed and published source code; ● Adoption of secure development practices aligned with OWASP SAMM, including secure coding, code reviews, and continuous integration security checks; ■ Testing and public scrutiny: <ul style="list-style-type: none"> ● Regular Public Intrusion Tests (PITs), with results made public and used to harden the system; ● A permanent public bug bounty program, allowing independent researchers to identify and report vulnerabilities; ■ Operational assurance, compliance, and monitoring: <ul style="list-style-type: none"> ● Operation under an ISO/IEC 27001:2022-certified Information Security Management System (ISMS), covering infrastructure and processes relevant to e-voting; ● Explicit compliance with the Federal Chancellery’s Ordinance on Electronic Voting (OEV), embedding its requirements into development, deployment, and operations.
Evidence	Security Whitepaper of the Swiss Post Voting System
Result	Pass
Finding	N/A
Relevance	N/A

Table 64 – 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	<p>The <i>Organizational concept</i> document “defines the structure, roles, and responsibilities of Swiss Post and its key stakeholders for the development, operation, and maintenance of the Swiss Post Voting System”.</p> <p>Roles are broken down into three categories:</p> <ul style="list-style-type: none"> ■ E-Voting Core Personnel; ■ Swiss Post Support and Infrastructure Teams; ■ External Suppliers and Service Providers. <p>A list of the personnel forming the core team is maintained up to date.</p> <p>People involved in the e-voting operations are instructed about their detailed responsibilities in specific training sessions.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting – Organizational concept (20/08/2025), §4, 6.2, 6.3 ■ E-Voting team – Mitarbeiterliste ■ E-Voting - Training concepts E-Voting (20/08/2025)
Result	Pass
Finding	N/A

Relevance	N/A
------------------	-----

Table 65 – 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	<p>The examiners understand that this requirement relates to the authorisation process for changes.</p> <p>Change management at the e-voting level follows the Post’s general change management process, which is based on ITIL best practices, and therefore includes an authorisation step.</p> <p>The e-voting-specific <i>Change and Maintenance Concept</i> provides additional details on the authorisation process for changes, depending on the operational phase of the system (e.g., green phase outside an election period, red phase in the run-up to an election).</p>
Evidence	<ul style="list-style-type: none"> ■ Change Management - Change Management – Richtlinie (20/08/2025) ■ E-Voting – Change and Maintenance Concept (20/08/2025), §4.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 66 – Examination results: OEV paragraph 18.2

Key	18.3
Requirement	The risks in connection with third parties (contractors irrespective of type, such as suppliers, service providers, etc.) 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	<p>The identification, analysis and treatment of supplier risks by Swiss Post are governed by the <i>Supplier Security Management policy Handbuch</i> document and complemented by an e-voting-specific concept. The concept lists the current suppliers mandated by Post CH Digital Services AG. PostFinance, the provider of the datacentre facilities for the e-voting infrastructure, is considered as forming an integral part of Swiss Post and is therefore not listed as a supplier.</p> <p>The process includes a four-category classification scheme of third parties depending on their risk profile. Based on the determined profile, several supplier risk assessment types may be performed:</p> <ul style="list-style-type: none"> ■ Onsite security assessment; ■ Remote security assessment; ■ Self-declarative assessment based on a specialised third-party software solution (Bitsight Cyber Risk Analytics & Security Ratings). <p>The classification also determines the frequency of the assessments to be performed. Contractual agreements with e-voting suppliers are based on Swiss Post’s general terms and conditions, which include confidentiality and data protection clauses, as well as a commitment to comply with Swiss Post’s internal regulations, “<i>in particular those relating to the information security, data protection and data security</i>”.</p> <p>Additional mandatory supplier security clauses are listed in the annex section of the policy.</p>
Evidence	<ul style="list-style-type: none"> ■ Handbuch Supplier Security Management V01.05

	<ul style="list-style-type: none"> ■ E-Voting - E-Voting Supplier Management (20/08/2025), §4 ■ https://www.post.ch/-/media/post/agb/kek/agb-dienstleistungen.pdf?vs=11&sc_lang=en, §4.5,11,12
Result	Pass
Finding	N/A
Relevance	N/A

Table 67 – Examination results: OEV paragraph 18.3

Management of intangible and tangible resources

Key	19.1
Requirement	<p>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.</p> <p>Swiss Post maintains a Configuration Management Database (CMDB) that includes all the components (a.k.a. Configuration Items or CI's) forming the e-voting system, including premises. They are all assigned a person who takes responsibility for it. It also maintains a catalogue of all its processes and keeps a list of its employees who are participating to the operation of the e-voting system.</p> <p>Swiss Post's quality management process requires regular reviews of the inventories to ensure they are up-to-date.</p>
Evidence	<ul style="list-style-type: none"> ■ Configuration & Asset Management - Configuration Management – Leitlinien (20/08/2025) ■ E-Voting team – Mitarbeiterliste ■ E-Voting – Organizational concept (20/08/2025), §5.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 68 – Examination results: OEV paragraph 19.1

Key	19.2
Requirement	The acceptable use of intangible and tangible resources must be defined.
Observation	<p>The Post maintains a general document regarding the acceptable use of assets, which is reviewed regularly.</p> <p>Employees are reminded regularly of the requirements of this document through security awareness campaigns.</p>
Evidence	<ul style="list-style-type: none"> ■ Sécurité de l'information à la place de travail: directive (29/08/2025) ■ Konzept Information Security Awareness V04.01
Result	Pass

Finding	N/A
Relevance	N/A

Table 69 – Examination results: OEV paragraph 19.2

Key	19.3
Requirement	Classification guidelines for information must be issued and communicated.
Observation	The <i>Classification of Information Factsheet</i> document defines the confidentiality, integrity, availability, and traceability levels governing the handling of business files, emails, and information in applications within Swiss Post. The <i>ISDS Konzept</i> for the e-voting system applies this classification by assigning confidentiality, integrity, availability, and traceability levels to the information processed by the system.
Evidence	<ul style="list-style-type: none"> ■ Classification of Information Factsheet ■ ISDS DS E-Voting (SDOC-3200417)
Result	Pass
Finding	N/A
Relevance	N/A

Table 70 – Examination results: OEV paragraph 19.3

Key	19.4
Requirement	Procedures must be devised for the labelling and handling of information.
Observation	The <i>Classification of Information Factsheet</i> document include instructions regarding the labelling and handling (storage, forwarding, input to generative AI solutions, handling physical information [paper]).
Evidence	Classification of Information Factsheet
Result	Pass
Finding	N/A
Relevance	N/A

Table 71 – 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	<p>The trustworthiness of Swiss Post's human resources interacting with the e-voting infrastructure is assessed through background checks in accordance with the established corporate HR process. The depth of the screening process depends on the risks associated with the position. E-voting employees are classified as category 2, which covers roles with direct or potential access to productive systems or sensitive data. In addition to the regular review of application files and references, joiners and movers must provide a criminal record extract. Employees in category 2 are also required to complete a periodic self-declaration covering significant financial issues or prior criminal convictions. In addition, random sample checks are conducted, requiring selected employees to provide an updated criminal record extract and debt collection register extract.</p> <p>All core team members (i.e., employees directly assigned to the e-voting programme) also sign Swiss Post's non-disclosure agreement, which remains valid after contract termination.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting – Organizational concept (20/08/2025), §6 ■ NDA Vorlage ■ Verbindliches Handbuch - Sicherheitsprüfungen von Mitarbeitenden (28/08/2025)
Result	Pass
Finding	N/A
Relevance	N/A

Table 72 – 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 <i>Manuel de Contrôle de sécurité du personnel</i> document states that the Swiss Post function <i>HR services 1st level</i> is responsible for the implementation and operation of the process "Personnel Security Control"
Evidence	Verbindliches Handbuch - Sicherheitsprüfungen von Mitarbeitenden (28/08/2025), p. 5
Result	Pass
Finding	Pass
Relevance	N/A

Table 73 – 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	<p>At corporate level, Swiss Post has established an information security awareness concept that pursues the following objectives:</p> <ul style="list-style-type: none"> ■ The importance of information security should be recognised; security should be taken seriously; ■ Security measures should be applied appropriately to their purpose, and correct behaviour should be instructed; ■ Ensure that Swiss Post's information security function is recognised as the first contact point for information security matters;

	<p>To implement this awareness concept, Swiss Post has put in place the following key measures:</p> <ul style="list-style-type: none"> ■ E-learning and campaigns: standardised videos and Web-Based Trainings delivered through the corporate Learning Management System to all staff, complemented by mandatory annual “Internet-Test” training for new and existing employees; ■ Interactive sessions: induction briefings, team workshops, and tailored contributions to internal events, complemented by innovative formats such as security “escape rooms”; ■ Phishing awareness: simulated phishing campaigns, an Outlook “report phishing” button, and supporting awareness material; ■ Just-in-time prompts: automated system warnings for risky actions (e.g., data leakage, etc.); ■ Active communication and resources: intranet news, employee magazine articles, regular security reporting, and self-service materials such as the “8 Golden Rules for Employees”. <p>Personnel interacting with the e-voting system are subject to specific onboarding sessions covering the e-voting infrastructure and its secure operation. Some training sessions are aimed at all employees involved in the e-voting project, while others are tailored to specific tasks and responsibilities and deepen technical or operational knowledge.</p>
Evidence	<ul style="list-style-type: none"> ■ Konzept Information Security Awareness V04.01, §2, 3 ■ E-Voting – Organizational concept (20/08/2025), §6.1.1 ■ E-Voting – Training concepts E-Voting (20/08/2025)
Result	Pass
Finding	N/A
Relevance	N/A

Table 74 – 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	Swiss Post’s <i>HB Sicherheitszonen – Die Schweizerische Post AG</i> document describes the company’s physical security perimeters, lists which type of premises belong to which security perimeter and defines the associated security requirements.
Evidence	HB Sicherheitszonen – Die Schweizerische Post AG V01.00, § 4.4, 5.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 75 – 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	<p>The e-voting system is hosted in Postfinance’s datacentres.</p> <p>The <i>Handbuch Zutrittsregelung PostFinance</i> document sets out the rules for the granting, assignment, management, and revocation of access rights to PostFinance premises.</p> <p>It is complemented by an annex (<i>Anhang 1 zu HB Zutrittsregelung: Betriebsstandorte PostFinance AG</i>), which sets out the specific technical and organisational measures for physical access control.</p> <p>The <i>Arbeitsanleitung Zutrittsverhalten Rechenzentren PostFinance AG</i> document defines the requirements for access behaviour to the system rooms of PostFinance AG.</p> <p>At Swiss Post level, the <i>Weisung Zutrittsmanagement</i> document lists the physical entry control requirements by security zone.</p>
Evidence	<ul style="list-style-type: none"> ■ Handbuch Zutrittsregelung PostFinance V04.00 ■ Anhang 1 zu HB Zutrittsregelung: Betriebsstandorte PostFinance AG ■ Arbeitsanleitung Zutrittsverhalten Rechenzentren PostFinance AG ■ KLA-Weisung Zutrittsmanagement «Die Schweizerische Post AG» V02.00, §5.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 76 – 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	<p>For this requirement, the examiners understand the term “devices” in a broad sense, covering both infrastructure components and end-user equipment.</p> <p>Swiss Post operates its e-voting system under an ISO/IEC 27001:2022-certified Information Security Management System (ISMS). This certification demonstrates that a comprehensive set of security controls, as defined in ISO/IEC 27002:2022, are applied systematically to safeguard devices and associated assets.</p> <p>The relevant ISO/IEC 27002 controls span across the four main categories of the standard:</p> <ul style="list-style-type: none"> ■ Organisational controls, e.g., policies, inventories, acceptable use rules, governance processes ensuring that devices are properly managed throughout their lifecycle; ■ People controls, e.g., screening, work agreements, awareness and training measures, etc., so that personnel are reliable, formally bound by their obligations, and sufficiently trained to understand their responsibilities and apply security requirements in daily work; ■ Physical controls: protection of infrastructure premises and equipment, including perimeter security, access restrictions, protection against hazards, visitor management, etc. Physical measures also extend to the secure storage, transfer, and disposal of hardware, ensuring that devices cannot be tampered with or misused; ■ Technological controls, e.g., secure configuration, patch and vulnerability management, network security measures, malware protection, data leakage prevention. monitoring of both endpoint devices and infrastructure components, etc., so that devices remain resilient against vulnerabilities, misuse, and external or internal attacks.

	Compliance with these controls is continuously monitored and periodically reviewed through the ISMS framework. This includes KPI collection, and analysis, internal audits, and annual certification audits. Management reviews further ensure that controls remain effective and aligned with the evolving threat landscape.
Evidence	<ul style="list-style-type: none"> ■ E-Voting – Organizational concept (20/08/2025), § 6.2 ■ ISO27001:2022 E-Voting Statement of Applicability, SoA (December 2024)
Result	Pass
Finding	N/A
Relevance	N/A

Table 77 – Examination results: OEV paragraph 21.3

Key	21.4
Requirement	All data must be processed and in particular stored exclusively in Switzerland.
Observation	<p>The e-voting system’s components operated by the Post are all stored in Postfinance’s datacentres located in Bern and Zofingen, Switzerland.</p> <p>However, the source code of the e-voting system as well as all the related documentation are hosted on the GitLab source code repository in the USA.</p> <p>Third-party libraries used by the e-voting front-end application are downloaded locally.</p>
Evidence	<ul style="list-style-type: none"> ■ Infrastructure Whitepaper of the Swiss Post Voting System ■ https://gitlab.com/swisspost-evoting
Result	Fail
Finding	The source code of the e-voting system as well as all the related documentation are hosted on the GitLab source code repository in the USA.
Relevance	The OEV should be more specific regarding the expression “all data” by specifying whether it includes the data not directly linked to voting events, such as the source code or technical logs for instance.

Table 78 – 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	<p>Risks originating from human resources relating to operations and communications may materialise through physical or logical access to the e-voting system components and include accidental behaviours (e.g., mishandling resulting in confidentiality, integrity or availability issues) as well as intentional malicious actions (e.g., fraud attempts, vandalism/sabotage, etc.).</p> <p>The <i>Organizational concept</i> document shows how areas of responsibility related to e-voting operations and communications are split between different teams, and how the four-eyes principle applied for the management of the components (control components, jumphosts, reverse proxy, front-end & back-end servers, databases) mitigates the risks of malicious actions.</p> <p>In terms of obligations, people involved in the e-voting operations and communications</p>

	are subject to HR screening, sign a non-disclosure agreement and must attend training sessions, which reduces the risk of both malicious actions and accidental behaviours. The risk report issued by Swiss Post related to the e-voting operations shows that risks originating from human resources are currently considered as acceptable (i.e. value <18) according to the criterion defined in the <i>Handbuch Risikomanagement</i> document.
Evidence	<ul style="list-style-type: none"> ■ E-Voting – Organizational concept (20/08/2025), § 6.2 ■ Whitepaper Infrastructure of the Swiss Post Voting System ■ E-Voting – Training concepts E-Voting (20/08/2025) ■ POST.DS6_Risikenauszug.Kantone_ ■ Handbuch Risikomanagement DS V04.01, §3.3.4
Result	Pass
Finding	N/A
Relevance	N/A

Table 79 – Examination results: OEV paragraph 22.1

Key	22.2
Requirement	Appropriate measures must be taken to protect against malware.
Observation	Protection against malware includes a wide range of measures, such as, e.g., 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, logging and monitoring, incident detection and response, etc. All these measures are part of Swiss Post’s Information Security Management System’s standard controls. This implies that the controls are formally documented, regularly reviewed, and subject to both internal and external audits, which provides assurance of their effective implementation and continuous improvement.
Evidence	ISO27001:2022 E-Voting Statement of Applicability, SoA (December 2024)
Result	Pass
Finding	N/A
Relevance	N/A

Table 80 – 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 plan for data backup is detailed within the <i>Data Backup Concept</i> document. It covers databases as well as application and system logs. The file system and application configuration are not backed up; they are redeployed through Infrastructure-as-Code (IaC) in case of recovery. The document details the type and frequency of restore tests performed (§2.7).
Evidence	E-Voting – Data Backup Concept (20/08/2025)
Result	Pass
Finding	N/A

Relevance	N/A
-----------	-----

Table 81 – 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	The Swiss Post network supporting the e-voting system falls within the scope of the company's ISO/IEC 27001-certified Information Security Management System, which aims at protecting the organisation's information assets in a systematic way, the effectiveness of which is regularly monitored and reviewed. In its <i>HB Network Security Architecture</i> document, Swiss Post has defined a set of sixteen security measures, each of which is broken down into specific implementation requirements. The <i>Infrastructure Whitepaper of the Swiss Post Voting System</i> document further details the high-availability properties of the e-voting system, which protect it against failures at both the network and network service levels. These measures mitigate the risks to network services identified under Number 13.
Evidence	<ul style="list-style-type: none"> ■ IT20 Workspace - HB Network Security Architecture (HNSA) (20/08/2025) - §7.1-7.16 ■ Infrastructure Whitepaper of the Swiss Post Voting System
Result	Pass
Finding	N/A
Relevance	N/A

Table 82 – 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	<p>In the context of e-voting operations, removable media include USB keys. These devices are used to exchange cryptographic material between Swiss Post and the cantons during the Direct Trust ceremony. A dedicated procedure specifies which USB key is to be used at each step of the ceremony for data transfer and requires that all devices be securely erased at the end of the process.</p> <p>The disposal of data carriers follows a formal process described in the <i>Übersicht Decommissioning von Hardware / Datenträgern</i> document. For USB keys, this process involves collecting the media in a lockable container that is securely handled by a specialised third-party company.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting collaboration platform - Direct Trust Zeremonie - R1.5 (28/10/2025), §6 ■ <i>Übersicht Decommissioning von Hardware / Datenträgern</i>
Result	Pass
Finding	N/A
Relevance	N/A

Table 83 – 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	<p>Change management at the e-voting level follows the Post's general change management process, which is based upon ITIL best practices and is complemented by e-voting-specific operational phases.</p> <p>The Post has defined two change phases for e-voting (red and green). During a ballot, change management enters a red phase in which modifications to the e-voting system are avoided as far as possible, except for predefined actions such as switching the landing-page phases. In exceptional circumstances, changes may still be required, for instance to address security-relevant issues or operational problems. The <i>E-Voting – Change and Maintenance Concept</i> document states that any proposed change during the red phase is reviewed and approved internally by several Swiss Post roles. As part of this review, the Product Owner – possibly in consultation with the Business Owner – must determine whether the change affects physical or logical access rights and therefore requires external stakeholders, such as the cantons or the Federal Chancellery, to be involved in the decision.</p>
Evidence	E-Voting – Change and Maintenance Concept (25/11/2025), §4.2, 4.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 84 – Examination results: OEV paragraph 23.1

Key	23.2
Requirement	<p>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.</p> <p>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.</p>
Observation	<p>The risk assessment performed by Swiss Post on the e-voting infrastructure includes mitigating measures (from the ISO27002:2022 standard) related to access control :</p> <ul style="list-style-type: none"> ■ A5.15 Access Control: contributes to the mitigation of six risks; ■ A5.18 Access Rights: contributes to the mitigation of six risks; ■ A7.1 Physical security perimeters: contributes to the mitigation of two risks; ■ A7.2 Physical entry: contributes to the mitigation of two risks; ■ A7.3: Security offices, rooms and facilities: contributes to the mitigation of one risk; ■ A7.4: Physical security monitoring: contributes to the mitigation of two risks. <p>From a general point of view, access control within Swiss Post is regulated by the Identity and Access Management (IAM) policy, which states the following principles relevant to this requirement:</p> <ul style="list-style-type: none"> ■ <i>“The approval process and the number of approval levels are defined on the basis of risk, depending on the risk classification of the IAM role. The risk classification determines whether, and how often, a recertification of the role assignment and role</i>

	<p><i>composition takes place”;</i></p> <ul style="list-style-type: none"> ■ <i>“The applicable authentication is determined by the risk classification of the entitlements through which access is obtained, as well as by the circumstances of access. The authentication process is dynamic and takes into account the risk profile of the access, the user’s behaviour, and contextual information”;</i> ■ <i>“All changes to role assignments and entitlements, as well as all changes to role compositions, are recorded. Changes to identities and their attributes are also recorded”;</i> ■ <i>“Every successful and failed authentication is recorded in an audit log. The login information must be adequately protected against modification and unauthorized access and must be retained for a sufficiently long period of time”.</i> <p>All physical and logical accesses to the e-voting components (reverse proxies, e-voting servers, control components) are performed in accordance with the four-eyes principle and are documented following change management good practices. These components constitute high-risk areas and are therefore subject to reinforced access control measures.</p> <p>Swiss Post is not directly involved in the manual operations in connection with the electronic ballot box, which are under the responsibility of the cantons. The operational guide of the e-voting platform shows that a password must be inputted by the e-voting authorities (AdminBoard, ElectoralBoard) to start the tallying process.</p> <p>The productive ballot boxes are automatically opened and closed according to the schedules defined by the administrators. However, the e-voting landing page must be activated to allow citizens to vote. This operation is carried out by a Swiss Post administrator through a formal change process that triggers an authentication procedure.</p>
Evidence	<ul style="list-style-type: none"> ■ POST.DS6_Risikenauszug.Kantone_, p. 120, 121 ■ Handbuch Identity and Access Management V02.00 ■ E-Voting – Security Elements Access Layer (20/08/2025), §6.10 ■ E-Voting – Security Elements Control Components (20/08/2025), §2.8 ■ E-Voting – Organizational Concept (20/08/2025), §6.1, 7, 9 ■ E-Voting - Release Management & Installation Concept (20/08/2025), §5, 6, 7 ■ Change and Maintenance Concept - E-Voting (20/08/2025), §4.1 ■ E-Voting collaboration platform - Benutzeranleitung Release 1.5, §5.1, 6.3.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 85 – 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	<p>This requirement may be broken down into two subcategories:</p> <ul style="list-style-type: none"> ■ Legitimate changes; ■ Illegitimate changes performed by internal and external malicious actors.

	<p>The e-voting system falls into the scope of the Post's ISO27001-certified Information Security Management System, which aims at protecting the organisation's information assets in a systematic way through a combination of policies and processes. Reducing the risk of illegitimate changes on the voting portal is performed through the implementation of various security best practices, e.g., secure development practices, vulnerability management, components hardening, access control, use of a Web Application Firewall, performance of regular technical tests (ethical hacking, public code review, etc.), logging and monitoring of activities combined with incident detection and response, etc.</p> <p>With regards to legitimate changes, the whole e-voting system, including the voting portal and related information pages, is subject to the Post's general change management process, which bases upon ITIL best practices, as well as to an e-voting specific change management process. Both of them require changes to be formally authorised.</p>
Evidence	<ul style="list-style-type: none"> ■ ISO27001:2022 E-Voting Statement of Applicability, SoA (December 2024) ■ Change Management - Change Management Richtlinie - (20/08/2025) ■ Change and Maintenance Concept - E-Voting (20/08/2025), §4.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 86 – 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	<p>This requirement may be broken down into two subcategories:</p> <ul style="list-style-type: none"> ■ Legitimate access; ■ Illegitimate access performed by malicious actors. <p>The e-voting system falls into the scope of the Post's ISO27001-certified Information Security Management System, which aims at protecting the organisation's information assets in a systematic way through a combination of policies and processes. Reducing the risk of illegitimate access to the infrastructure during a ballot is achieved through the implementation of various security best practices, e.g., physical and logical access control, privileged access management, secure development practices, vulnerability management, components hardening, use of a Web Application Firewall, performance of regular technical tests (ethical hacking, public code review, etc.), logging and monitoring of activities combined with incident detection and response, etc.</p> <p>With regards to legitimate changes, Swiss Post has defined two change phases for e-voting (red and green). When a ballot takes place, change management enters a red phase, where changes are frozen by default. The process strictly limits changes to emergencies. during the red period, e.g., in case of incident.</p>
Evidence	<ul style="list-style-type: none"> ■ ISO27001:2022 E-Voting Statement of Applicability, SoA (December 2024) ■ Change and Maintenance Concept - E-Voting (20/08/2025), §4.5
Result	Pass
Finding	N/A

Table 87 – 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	<p>The examiners understand that this requirement applies to the authentication process of voters on the voting portal.</p> <p>At the infrastructure level, TLS v1.3 is implemented to prevent the interception of credentials transmitted from the voters' endpoints to the voting portal (a.k.a man-in-the-middle attacks).</p> <p>Likely redirection scenarios include the following:</p> <ul style="list-style-type: none"> ■ Social engineering attacks (e.g., submission of a forged URL that the voter believes to be genuine). Such an attack may be more effective if the legitimate voting portal is vulnerable to specific application flaws (e.g., Open redirect, cross site scripting, etc.). In that case, the forged link would still point to the right domain name; ■ DNS poisoning attacks. <p>The voting material includes the fingerprint of the voting portal and instructs voters to check it to ensure that they have not been redirected to a malicious website.</p> <p>DNS poisoning is mitigated by the implementation of DNSSEC. It is to note that the protection measure becomes effective only if the voters' internet service providers are themselves implementing DNSSEC.</p> <p>Other countermeasures include secure development practices, use of a Web Application Firewall, performance of regular technical tests (ethical hacking, public code review, etc.).</p> <p>From a general point of view, the e-voting system falls into the scope of the Post's ISO27001-certified Information Security Management System, which aims at protecting the organisation's information assets in a systematic way through a combination of policies and processes. This includes in particular the protection of authentication credentials.</p> <p>Abuse of authentication means includes various attack types, such as stealing, guessing or brute-forcing of credentials, abuse of password recovery functions, session prediction, etc.</p> <p>The e-voting system supports two modes of authentication: either directly on the voting portal or by implementing identity federation with a canton's existing Identity Provider. In the former case, most countermeasures result from secure design principles at the application level which is out of the present examination scope. In the latter case, the responsibility for protecting the authentication function is assumed by the canton.</p>
Evidence	<ul style="list-style-type: none"> ■ ISO27001:2022 E-Voting Statement of Applicability, SoA (December 2024) ■ E-Voting – Security Elements Access Layer (20/08/2025), §4, 6.2 ■ Security advices
Result	Pass
Finding	N/A
Relevance	N/A

Table 88 – Examination results: OEV paragraph 23.5

Development and maintenance of information systems

Key	24.2.1
------------	--------

Requirement	<p>An operating manual is created that includes the following for each user role:</p> <ul style="list-style-type: none"> ■ a description of the functions that the user can access and the permissions that must be controlled in a secure environment, including appropriate warnings; ■ a description of how the available interfaces can be used in a secure manner; ■ a description of the available functions and interfaces, in particular all security parameters under the control of the user, highlighting the values relevant to security; ■ a precise description of all types of security events related to the user-accessible functions to be performed, including adjustments to the security properties of elements under the control of the security functions; ■ a description of the security measures to be implemented in order to achieve the operational security objectives.
Observation	<p>Swiss Post maintains an operational guide (<i>Benutzeranleitung</i>) of its e-voting system. The document is structured sequentially according to the chronological phases of an electronic voting process. Each chapter corresponds to one operational stage, from the preparation of the election event to the deletion of data after the vote.</p> <p>The document is primarily intended for cantonal administrators and members of the election authority. It provides procedural instructions for each step, including system preparation, data exchange between offline and online components, conduct of the electronic vote, tallying, and data deletion.</p> <p>It identifies the main user roles: E-voting administrator (admin board), election authority (electoral board), whose activities are described throughout the operational phases (e.g., election setup, sealing and unsealing of electronic urns, tallying, etc.). Voters are mentioned only in relation to certain messages or operational conditions (e.g. system outage) but no specific user activities or functions are documented for them.</p> <p>It provides implicit and procedural security warnings, e.g., handling of PIN-protected data carriers, verification of digital certificates, integrity checks of cryptographic material, etc.</p> <p>The operational instructions provided are designed in accordance with good security practices. Each procedure involving system interfaces includes steps that ensure secure handling and integrity of the exchanged information.</p> <p>The guide also embeds scattered instructions contributing to secure operation, such as isolation of components, physical separation of roles, use of PINs, checksum verification, and controlled restoration from backups.</p> <p>Swiss Post's operating manual largely fulfils the intent of requirement 24.2.1 by providing detailed, step-by-step instructions that ensure operational tasks are performed securely and consistently. However, the guide does not include a role–function matrix specifying which functionalities are accessible to each type of user, nor does it provide a structured overview of all security-relevant events associated with user-accessible functions.</p>
Evidence	E-Voting collaboration platform – Benutzeranleitung Release 1.5
Result	Partially fail
Finding	Swiss Post's operating manual does not include a role–function matrix specifying which functionalities are accessible to each type of user, nor does it provide a structured overview of all security-relevant events associated with user-accessible functions.
Relevance	From a practical perspective, achieving full alignment with the literal wording of the requirement would likely reduce the document's usability, as the operational guide is designed to be procedural and actionable rather than an exhaustive reference document. In the examiners' opinion, the current level of detail is therefore consistent with the document's operational purpose, while still supporting secure execution of all

	described tasks.
--	------------------

Table 89 – Examination results: OEV paragraph 24.2.1

Key	24.2.2
Requirement	The operating manual must identify all possible modes of operation of the software, including the resumption of operation after the detection of errors and the description of the consequences and effects of errors on the maintenance of secure operation.
Observation	<p>Swiss Post’s operational manual describes the operational modes of the e-voting system through the successive phases of an election – preparation (D0), configuration (D1–D2), voting (EV), tallying (D3), and data deletion (D4).</p> <p>Each phase corresponds to a specific operational state of the system, supported by distinct components (PC-Setup, PC-Online, PC-Tally, PC-Verifier, etc.). These descriptions collectively identify the main modes of operation.</p> <p>The document succinctly outlines the actions to be taken when a system outage occurs (Section § 5.5: <i>Vorgehen bei Systemausfall</i>). The instructions are high-level and do not detail technical steps or security implications.</p> <p>The <i>Emergency Concept</i> document complements these instructions by defining specific failure scenarios and corresponding recovery measures. It describes how operations can be resumed after outages affecting different components</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting collaboration platform – Benutzeranleitung Release 1.5, §5.5 ■ E-Voting – Emergency Concept (20/08/2025), §5
Result	Pass
Finding	N/A
Relevance	N/A

Table 90 – Examination results: OEV paragraph 24.2.2

Key	24.2.3
Requirement	The operating manual must be precise and fit for purpose.
Observation	<p>The operating guide is clearly structured according to the chronological phases of an election and provides step-by-step procedural instructions for each activity. The instructions are written in operational language, aligned with the tasks of cantonal administrators and the election authority, and supported by consistent terminology, screenshots and contextual information boxes. The guide is therefore precise and practical for its intended users.</p> <p>Certain sections, such as error handling (§ 5.5), remain high-level, reflecting the document’s operational purpose rather than technical depth. The guide is also subject to continuous improvement and readability efforts, demonstrating Swiss Post’s commitment to maintaining documentation that is both accurate and accessible.</p> <p>Overall, the guide is fit for purpose as a procedural manual, offering sufficient detail to perform the described tasks securely and consistently.</p>
Evidence	E-Voting collaboration platform – Benutzeranleitung Release 1.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 91 – Examination results: OEV paragraph 24.2.3

Key	24.3.1
Requirement	The preparation process describes all the steps necessary for: <ul style="list-style-type: none"> ■ the secure acceptance of the system components in accordance with the delivery procedure; ■ the secure preparation of the operating environment in accordance with the operational security objectives; ■ the secure installation of the software in the operating environment.
Observation	The <i>Release Management & Installation Concept</i> document defines the steps ensuring the secure acceptance of system components, the secure preparation of the operating environment, and the secure installation of the software. The process applies consistently across all layers of the system – hardware, operating system, and application. For hardware, installations are performed under the four-eyes principle and documented through signed checklists and acceptance protocols, ensuring integrity and traceability. Operating systems are freshly installed at regular intervals using approved and hardened images, with configuration controls enforced through documented procedures and peer validation. Application components are deployed exclusively from the internal artifact repository, using Infrastructure as Code and verified hash values to ensure software integrity. Each installation follows a standardized checklist, and final validation is conducted as part of a Trusted Deployment ceremony with independent witnesses.
Evidence	E-Voting - Release Management & Installation Concept (20/08/2025)
Result	Pass
Finding	N/A
Relevance	N/A

Table 92 – Examination results: OEV paragraph 24.3.1

Key	24.3.2
Requirement	The delivery of the software or parts of the system must be documented and include all processes required to maintain security in the delivery of the software
Observation	The <i>Release Management & Installation Concept</i> describes a well-documented and controlled process ensuring the secure delivery of software and system components. All deliveries are performed through internal, trusted channels within Swiss Post's secured infrastructure, excluding any direct internet connections for trustworthy components. Software packages and images are stored, versioned, and distributed exclusively via the internal Artifact repository manager, which ensures authenticity and integrity through cryptographic hash verification. Each delivery and deployment is associated with a formal IT change record, linked to detailed checklists and step-by-step documentation, guaranteeing full traceability of every action performed. Communication and coordination between teams are managed through dedicated project and change management tools, ensuring transparency and accountability.
Evidence	E-Voting - Release Management & Installation Concept (20/08/2025), §6, 7, 8
Result	Pass
Finding	N/A
Relevance	N/A

Table 93 – Examination results: OEV paragraph 24.3.2

Key	24.3.3
Requirement	<p>A reliable and verifiable compilation with appropriate security measures must be carried out. This ensures that the executable code is a verifiable and faithful representation of the source code which has been subjected to public scrutiny and independent examinations. The compilation allows a chain of proofs to be created for the verification of the software and includes in particular:</p> <ul style="list-style-type: none"> ■ evidence that the compilation environment is designed as described on the public platform (all tools with the respective version, operating system and any configurations); any derogations must be documented and justified; ■ evidence that the software has been compiled in accordance with the instructions available on the public platform; if an error in the instructions is found during compilation, this must be recorded and the documentation must subsequently be corrected; ■ evidence that the source code submitted for public scrutiny and examined is in fact the source code used for compilation; ■ evidence that no elements other than those provided for in the instructions have been introduced; ■ evidence that the cryptographic signature of all dependencies has been verified against a proven, public, and trusted reference (e.g. Maven Central Repository); ■ evidence that a dependency vulnerability analysis has been performed and that, if vulnerabilities relevant to the software exist, they do not render the software vulnerable to attack; ■ evidence that the parameters introduced, if any, do not render the system vulnerable.
Observation	<p>Swiss Post has implemented a Trusted Build concept, which defines a controlled and reproducible compilation process ensuring that the executable code is a verifiable and faithful representation of the publicly reviewed source code.</p> <p>The process is conducted by independent experts who perform a full compilation of the e-voting software using the publicly available source code, build scripts, and configuration files.</p> <p>Upon completion, the experts record the cryptographic hash values of all resulting artifacts and digitally sign the corresponding Trusted Build Protocol.</p> <p>These signed protocols are published in the public GitLab repository, enabling external auditors, cantonal authorities, and any interested party to independently verify that the compiled binaries exactly match the examined source code.</p> <p>The build environment is strictly controlled and documented, including the definition of the operating system, compiler versions, and supporting tools required for reproducible builds.</p> <p>Integrity and authenticity checks are systematically applied:</p> <ul style="list-style-type: none"> ■ Cryptographic signatures of all dependencies are verified against trusted public repositories ■ A dependency vulnerability analysis is performed to ensure that any known weaknesses in third-party components do not render the compiled software vulnerable. ■ Only approved third-party components, validated by Swiss Post's architecture and security groups, may be used in the build process. <p>This approach creates a transparent chain of evidence from the publicly disclosed source code to the independently verified executable, satisfying the requirement for reliable, reproducible, and verifiable compilation with appropriate security measures.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting - Release Management & Installation Concept (20/08/2025), §8 ■ Trusted Build and Trusted Deployment of the Swiss Post Voting System

	<ul style="list-style-type: none"> ■ Secure Software Development Process of the Swiss Post Voting System ■ Protocols (R1.4.5.1)
Result	Pass
Finding	N/A
Relevance	N/A

Table 94 – Examination results: OEV paragraph 24.3.3

Key	24.3.4
Requirement	<p>A reliable and verifiable deployment with appropriate security measures must be carried out. This is to ensure that:</p> <ol style="list-style-type: none"> 1. the code used in production is a verifiable and faithful representation of the source code which has been subjected to public scrutiny and independent examinations; and 2. the production environment conforms to that which has been subjected to public scrutiny and independent examinations. <p>The deployment allows a chain of proofs to be created for the verification of the software and includes in particular:</p> <ul style="list-style-type: none"> ■ evidence that the production environment is the same as that which has been subjected to public scrutiny and independent examinations; any discrepancies (firmware version, configuration files, etc.) must be documented and justified; ■ evidence that the software deployed in the production environment is in fact that which was created using a reliable and verifiable compilation process; ■ evidence that the parameters introduced, if any, do not render the system vulnerable.
Observation	<p>Swiss Post applies a structured and traceable deployment process ensuring that the software executed in production faithfully corresponds to the version that has undergone public scrutiny and independent examination. The trusted deployment uses as input the trusted build protocols digitally signed by the independent experts. These protocols confirm that the compiled binaries correspond to the reviewed source code and were reproducibly generated through the trusted build process.</p> <p>The deployment is performed during a formal ceremony attended by Swiss Post operators and independent experts. During this process, the observers verify that the frontend and backend applications deployed on Swiss Post’s infrastructure match the cryptographic hashes recorded in the trusted build protocol. They also check that the configuration of the production environment, including operating system versions and component settings, conforms to the technical specifications published for independent review. Following these verifications, the independent experts sign an acceptance protocol confirming the correspondence between the deployed software and the trusted build artifacts. Swiss Post publishes this signed protocol in the public repository, ensuring transparency and traceability.</p> <p>Once the deployment is completed, Swiss Post operators lose access to the production systems until the end of the election event, preventing any subsequent modification of the approved configurations or binaries.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting - Release Management & Installation Concept (20/08/2025), §8 ■ Trusted Build and Trusted Deployment of the Swiss Post Voting System ■ Secure Software Development Process of the Swiss Post Voting System ■ Protocols (R1.4.5.1)
Result	Pass
Finding	N/A

Relevance	N/A
-----------	-----

Table 95 – Examination results: OEV paragraph 24.3.4

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 scientific knowledge and experience
Observation	<p>Swiss Post publishes the protocols of the trusted build exercise performed both by the cantons and an external contracted company.</p> <p>The deployment of the e-voting software takes place during a formal ceremony attended physically by Swiss Post operators in the presence of independent experts. These experts verify that the frontend and backend applications deployed on Swiss Post’s infrastructure correspond exactly to the cryptographic hashes recorded in the trusted build protocol. Once verification is complete, the experts sign an acceptance protocol confirming that the observed hashes match those specified in the trusted build documentation.</p> <p>The signed acceptance protocol is then published in the public source code repository, providing transparent and verifiable evidence of the independent witnessing of the deployment.</p> <p>The reproducible build and public release of source code, dependencies, and instructions allow any third party to independently verify the build and compare hash values. This enables scientifically verifiable proof of software authenticity, even without physical witnesses.</p>
Evidence	<ul style="list-style-type: none"> ■ Trusted build protocols ■ Secure Software Development Process of the Swiss Post Voting System ■ E-Voting Trusted Deployment Acceptance Protocol – July 2025
Result	Pass
Finding	N/A
Relevance	N/A

Table 96 – 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	<p>The chain of evidence for reliable and verifiable compilation and deployment is composed of the trusted build protocols and the trusted deployment acceptance protocols.</p> <p>These signed and published documents are publicly available on Swiss Post’s e-voting GitLab repository, ensuring full transparency and independent verifiability.</p>
Evidence	Trusted build protocols
Result	Pass
Finding	N/A
Relevance	N/A

Table 97 – Examination results: OEV paragraph 24.3.6

Key	24.4.1
Requirement	<p>Processes are defined for the correction of flaws. The processes include:</p> <ul style="list-style-type: none"> ■ 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	<p>Swiss Post operates a public bug bounty programme through the <i>YesWeHack</i> platform, enabling independent researchers to responsibly disclose vulnerabilities. The programme is presented on a dedicated public web page describing its objectives, scope, and the mechanisms available for external experts to review the system and report vulnerabilities.</p> <p>Reported flaws and their resolution are tracked in the public e-voting GitLab repository, where the issue tracker contains individual entries with timestamps, descriptions, discussion threads, and status updates.</p> <p>In some cases, issues also reference merge requests or commits associated with the corresponding fixes.</p>
Evidence	<ul style="list-style-type: none"> ■ Bug bounty programme ■ Swiss Post e-voting community programme ■ List of opened issues
Result	Pass
Finding	N/A
Relevance	N/A

Table 98 – Examination results: OEV paragraph 24.4.1

Key	24.4.2
Requirement	<p>A process is defined for handling reported flaws.</p> <p>This process ensures that all reported and confirmed flaws are corrected and that the procedures for correction are communicated to system users.</p> <p>It provides for arrangements to ensure that the correction of security flaws does not give rise to new security flaws.</p>
Observation	<p>The handling of reported flaws affecting the e-voting software is performed through the bug bounty process operated on the <i>YesWeHack</i> platform.</p> <p>Public visibility of reported and confirmed flaws is provided through the Swiss Post e-voting GitLab issue tracker where open and closed issues are documented with timestamps, descriptions, and status updates.</p> <p>The issue tracker includes a <i>Description</i> field detailing how each reported vulnerability is to be addressed and a <i>Status</i> field indicating when the issue has been resolved.</p> <p>This ensures traceability and a public record of the corrective actions applied to reported flaws.</p>

	<p>To prevent the introduction of new flaws during remediation, Swiss post applies controls for implementing code changes. All modifications are submitted as pull requests and undergo peer review under the four-eyes principle.</p> <p>For cryptographically sensitive components, a specialist review is required.</p> <p>Additionally, static code analysis tools and automated test pipelines are applied before any merge to the main branch.</p> <p>These measures ensure that corrective actions do not introduce new vulnerabilities into the system.</p>
Evidence	<ul style="list-style-type: none"> ■ Bug bounty programme ■ List of opened issues ■ Software development process of the Swiss Post voting system
Result	Pass
Finding	N/A
Relevance	N/A

Table 99 – Examination results: OEV paragraph 24.4.2

Key	24.4.3
Requirement	<p>Policies must be defined for the reporting and correction of flaws. These include:</p> <ul style="list-style-type: none"> ■ instructions on how system users can report suspected security flaws to the developer; ■ instructions on how system users can register with the developer to receive reports of security flaws and the corrections; ■ details of specific contact points for all reports and inquiries on security issues concerning the software.
Observation	<p>The Swiss Post e-voting community Programme web page defines the public channels and policies for reporting and correcting software flaws. It explicitly informs external researchers how to submit vulnerability reports (notably via the public bug-bounty programme on <i>YesWeHack</i>) and points to the public GitLab repository where findings, protocols and remediation activity are published. The page also provides contact mechanisms for enquiries, a registration page for newsletter subscriptions, and directs interested parties to the community portal and GitLab as the authoritative locations for published reports and updates.</p>
Evidence	Swiss Post e-voting community programme
Result	Pass
Finding	N/A
Relevance	N/A

Table 100 – Examination results: OEV paragraph 24.4.3

Operation

Key	25.6.2
Requirement	Persons who operate and use the system must be trained and provided with the necessary documentation

Observation	<p>Swiss Post provides training to its employees involved in the operation of the e-voting system as well as to the cantons. The <i>Training concepts E-Voting</i> document details the types of training provided to employees according to their role:</p> <ul style="list-style-type: none"> ■ All employees receive training covering the basic understanding of Swiss Post applications and internal standards, as well as awareness on security, compliance and data protection; ■ In addition, persons involved in the e-voting operations are trained on understanding the e-voting system architecture and its components, project-specific processes and responsibilities, and preparation for audits and secure record keeping; ■ Finally, role-specific advanced training is provided for specialised functions. <p>Training-related documentation is maintained in accordance with Swiss Posts's quality and document management processes.</p> <p>Regarding cantonal users, Swiss Post provides formal training for cantonal system administrators responsible for operating the e-voting system.</p> <p>Up to ten administrators per canton participate in a structured administrator training programme, which covers the complete process of setting up, conducting, and finalising an election using the Swiss Post e-voting solution.</p> <p>This training ensures that administrators are able to independently perform all operational steps of an election.</p> <p>As part of the base service, the training is conducted once per integration project and includes the delivery of comprehensive training materials.</p> <p>Additional training and practical experience are provided during the end-to-end testing phase, enabling administrators to familiarise themselves with the live operational workflow.</p> <p>The Operational Guide (<i>Benutzeranleitung</i>) serves as the main document for users of the e-voting application.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting – Training concepts E-Voting (20/08/2025) ■ E-Voting – Organizational concept (20/08/2025), §5.1 ■ Dienstleistungsrahmenvertrag - Anhang A: Servicebeschreibung (21.12.2021), §4.1 ■ E-Voting collaboration platform - Benutzeranleitung Release 1.5
Result	Pass
Finding	N/A
Relevance	N/A

Table 101 – Examination results: OEV paragraph 25.6.3

Key	25.6.3
Requirement	Training includes the opportunity to train on a system designed for training purposes.
Observation	<p>The <i>training concepts E-Voting</i> document states that training on e-voting topics for Swiss Post employees takes place on a dedicated training platform, unless access to production environments is explicitly required.</p> <p>The <i>Servicebeschreibung</i> document mentions hands-on training for cantonal administrators, including the execution of all steps of an election during the end-to-end integration tests. The training is conducted on a dedicated server-side training environment specifically prepared, deployed, and configured for this purpose.</p>
Evidence	<ul style="list-style-type: none"> ■ E-Voting – Training concepts E-Voting (28/10/2025) ■ Dienstleistungsrahmenvertrag - Anhang A: Servicebeschreibung (21.12.2021), §4.2
Result	Pass

Finding	N/A
Relevance	N/A

Table 102 – Examination results: OEV paragraph 25.6.3

Key	25.6.4
Requirement	Help on using the system must be readily available.
Observation	<p>The Operational Guide (<i>Benutzeranleitung</i>) is the main document providing help on using the system.</p> <p>The Post has also developed a dedicated collaboration platform on e-voting with the cantons, including frequently asked questions (FAQ's) and help checklists.</p> <p>Every canton has access to the e-voting competence centre, either via e-mail or phone. Each canton is allocated a Single Point of Contact (SPOC).</p>
Evidence	<ul style="list-style-type: none"> ■ Dienstleistungsrahmenvertrag - Anhang A: Servicebeschreibung (21.12.2021), §4.1 ■ Evoting collaboration platform: https://wiki.post.ch/spaces/EVOCP/
Result	Pass
Finding	N/A
Relevance	N/A

Table 103 – Examination results: OEV paragraph 25.6.4

5 Summary of findings and recommendations

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

Key	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	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.
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 canton. 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. The Federal Chancellery has explicitly authorised the Direct Trust approach for the cantons, making this deviation compliant at the regulatory level. Therefore, no further action is required in the examiners' opinion.

Table 104 – Finding related to OEV paragraph 15.4

Key	21.4
Requirement	All data must be processed and in particular stored exclusively in Switzerland.
Finding	The source code of the e-voting system as well as all the related documentation are hosted on the GitLab source code repository in the USA.
Recommendation	During previous audits, Swiss Post has already confirmed that it does not intend to migrate the hosting of its source code or documentation away from GitLab, as these elements are not considered part of the election data that must remain in Switzerland. Although the requirement is not met under a strict literal reading, the deviation has no material impact on the security or trustworthiness of the voting process. No corrective action is required in the examiners' opinion.

Table 105 – Finding related to OEV paragraph 21.4

Key	24.2.1
Requirement	An operating manual is created that includes the following for each user role: <ul style="list-style-type: none"> ■ a description of the functions that the user can access and the permissions that must be controlled in a secure environment, including appropriate warnings; ■ a description of how the available interfaces can be used in a secure manner; ■ a description of the available functions and interfaces, in particular all security parameters under the control of the user, highlighting the values relevant to security;

	<ul style="list-style-type: none"> ■ a precise description of all types of security events related to the user-accessible functions to be performed, including adjustments to the security properties of elements under the control of the security functions; <p>a description of the security measures to be implemented in order to achieve the operational security objectives.</p>
Finding	<p>Swiss Post’s operating manual does not include a role–function matrix specifying which functionalities are accessible to each type of user, nor does it provide a structured overview of all security-relevant events associated with user-accessible functions.</p>
Recommendation	<p>From a practical perspective, achieving full alignment with the literal wording of the requirement would likely reduce the document’s usability, as the operational guide is designed to be procedural and actionable rather than an exhaustive reference document. In the examiners’ opinion, the current level of detail is therefore consistent with the document’s operational purpose, while still supporting secure execution of all described tasks.</p>

6 References

- [1] “Swiss Citizens should be able to vote electronically,” Administration numérique suisse, [Online]. Available: <https://www.digital-public-services-switzerland.ch/en/implementation/egovernment-implementation-plan/redesigning-evoting>. [Accessed 22 May 2024].
- [2] “Redesign and relaunch of trials - Final report of the Steering Committee Vote électronique (SC VE),” Swiss Federal Chancellery, Political Rights Section, 30 November 2020. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/Final%20report%20SC%20VE_November%202020.pdf.download.pdf/Final%20report%20SC%20VE_November%202020.pdf. [Accessed 22 May 2024].
- [3] “Partial revision of the Ordinance on Political Rights and total revision of the Federal Chancellery Ordinance on Electronic Voting (Redesign of Trials),” Swiss Federal Chancellery, Political Rights Section, 28 April 2021. [Online]. Available: <https://www.bk.admin.ch/dam/bk/en/dokumente/pore/Explanatory%20report%20for%20consultation%202021.pdf.download.pdf/Explanatory%20report%20for%20consultation%202021.pdf>. [Accessed 22 May 2024].
- [4] “Federal Chancellery Ordinance on Electronic Voting (OEV),” Swiss Federal Chancellery, 21 April 2021. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/OEV_draft%20for%20consultation%202021.pdf.download.pdf/OEV_draft%20for%20consultation%202021.pdf. [Accessed 22 May 2024].
- [5] “Audit concept v1.3 for examining Swiss Internet voting systems,” Federal Chancellery (FCh), Political Rights Section, 18 May 2021. [Online]. Available: <https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Audit%20concept,%2018.05.2021.pdf.download.pdf/Audit%20concept,%2018.05.2021.pdf>. [Accessed 22 May 2024].
- [6] “Examination of the Swiss Internet voting system, Version:1.0 / Audit scope: Infrastructure and operations (3) – Measures of the System Provider,” Swiss federal chancellery, March 2022. [Online]. Available: <https://www.newsd.admin.ch/newsd/message/attachments/71144.pdf>. [Accessed 16 July 2024].
- [7] “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].

- [8] “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].
- [9] “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--electronique/Audit%20concept%20v1.5.pdf.download.pdf/Audit%20concept%20v1.5.pdf>. [Accessed 22 May 2024].
- [10] “Examination of the Swiss Internet voting system, Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the system provider - Round 2,” SCRT, November 2022. [Online]. Available: [https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_Reports_March2023/Scope%203%20\(Post\)%20Final%20Report%20SCRT%2028.11.2022.pdf.download.pdf/Scope%203%20\(Post\)%20Final%20Report%20SCRT%2028.11.2022.pdf](https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_Reports_March2023/Scope%203%20(Post)%20Final%20Report%20SCRT%2028.11.2022.pdf.download.pdf/Scope%203%20(Post)%20Final%20Report%20SCRT%2028.11.2022.pdf). [Accessed 16 July 2024].
- [11] “Examination of the Swiss Internet voting system, Version: 1.0 / Audit scope: Infrastructure and operations (3) – Measures of the system provider - Round 3 & changes,” SCRT, June 2023. [Online]. Available: [https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_reports_August2023/Scope%203%20\(Post\)%20Final%20Report%20SCRT%2016.06.2023.pdf.download.pdf/Scope%203%20\(Post\)%20Final%20Report%20SCRT%2016.06.2023.pdf](https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_reports_August2023/Scope%203%20(Post)%20Final%20Report%20SCRT%2016.06.2023.pdf.download.pdf/Scope%203%20(Post)%20Final%20Report%20SCRT%2016.06.2023.pdf). [Accessed 16 July 2024].
- [12] “Examination of the Swiss Internet voting system, Version 1.0 / Audit scope: Infrastructure and operations (3) - Measures of the system provider,” Orange Cyberdefense Switzerland, 19 August 2024. [Online]. Available: [https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_reports_August2024/Scope%203%20\(Cantons\)%20Final%20Report%20Orange%20Cyberdefense%20\(SCRT\)%2012.07.2024.pdf.download.pdf/Scope%203%20\(Cantons\)%20Final%20Report%20Orange%20Cyberdefense%2012.07.2024.pdf](https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_reports_August2024/Scope%203%20(Cantons)%20Final%20Report%20Orange%20Cyberdefense%20(SCRT)%2012.07.2024.pdf.download.pdf/Scope%203%20(Cantons)%20Final%20Report%20Orange%20Cyberdefense%2012.07.2024.pdf). [Accessed 18 August 2025].
- [13] “Audit concept v1.6 for examining Swiss internet voting systems,” Federal Chancellery (FCh), Political Rights Section, 7 February 2025. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Audit%20concept%20v1.6.pdf.download.pdf/Audit%20concept%20v1.6.pdf. [Accessed 21 July 2025].