SCRT
Information Security

Examination of the Swiss Internet voting system

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

26/03/2022

Work performed for:

Swiss Federal Chancellery
Political Rights Section
Federal Palace West Wing
3003 Bern

Contact information

SCRT SA
Rue du sablon 4
1110 Morges
Switzerland

Stéphane Adamiste
Head of Governance division
+41 21 802 64 01
stephane.adamiste@scrt.ch

Contributors

Author	Stéphane Adamiste	Head of Governance division
Reviewer	Antonio Fontes	Head of Cloud security division
Reviewer	Sergio Alves Domingues	Chief Technology Officer

Version history

Version Number	**Author**	**Date**	**Version**
0.9	Stéphane Adamiste	26.02.2022	Draft for review
0.91	Stéphane Adamiste	07.03.2022	Improved version following questions and comments by Federal Chancellery
1.0	Stéphane Adamiste	26.03.2022	Final version following comments by Post

Management summary

Scope and objective of the examination

The objective of this examination was to assess to which extent the Swiss Post's infrastructure and organisational measures supporting its e-voting system satisfies a subset of requirements (audit 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 e-voting. In total, the examination included 73 criteria.

Methodology

The examiners looked for evidence of effort to comply with said criteria by performing interviews of the Swiss Post's personnel in charge of the setup and operation of the e-voting system's infrastructure, and by analysing the relating documentation (i.e., policies, procedures, specifications, reports, processes, etc.).

The examination was performed mostly from mid-September to mid-November 2021. Some complementary interviews were conducted in January and early February 2022. The total workload for this examination, including the edition of this report, is 180 hours.

Results

Twenty-four non-compliances (findings) were identified and reported.

From a general point of view, the examiners could observe a large amount of effort deployed by the Swiss Post to meet the requirements of the ordinance on e-voting. It encompasses both good practices inherited from the company's ISO27001 certified Information Security Management System (ISMS), and specific measures implemented by the e-voting teams. In particular, a consequent documentation effort, by the latter teams, of their processes and procedures, was noted.

Observed non-compliances were found to have the following origins:

- In some instances, the examinee has not yet formalised some processes required by the ordinance. Notable examples include the installation procedure of the e-voting software on the control components, or the reliable and verifiable e-voting software deployment process;
- Some activities supposed to be carried out as part of the company's ISMS have not been conducted at the e-voting level, or are not finalised yet, or miss some specificities required by the ordinance. For example, the supplier security management process does not seem to have been applied to the e-voting supply chain; the Information Security and Data Privacy concept, which serves as input for the assessment of the risks pertaining to the e-voting system, is not finalised and fails to provide a detailed level of analysis at some points, that could help better demonstrating compliance with the ordinance;
- Some supporting documentation is missing or is not up to date, leading to a lack of evidence, and obsolete and/or irrelevant information. In particular, the *operational guide* document does not include several of the required elements.

- One requirement does not seem to be achievable and should be reconsidered.

Recommendations

Only succinct recommendations are provided in this document, as the observations formulated are self-explanatory in most of the cases. Implementation of those recommendations requires a moderate effort at the scale of the e-voting project in the examiners' opinion.

This report provides also comments at the attentions of the Federal Chancellery when the examination criteria were perceived as unclear, or subject to interpretation.

Final note

The examiners conclude this summary by thanking the Swiss Post, and more particularly all the personnel that has been involved, for its cooperation and for the transparency demonstrated throughout the entire duration of the examination.

Table of content

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 Swiss Post of the withdrawal of its e-voting system from operation to focus on improving the solution. Since then, e-voting is 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, using "e-voting systems, which are fully verifiable" [1]. This redesign of the trial phase focuses on four objectives:

   1. Further development of the e-voting systems
   2. Effective controls and monitoring
   3. Increased transparency and trust
   4. 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. In April 2021, the Federal Council opened a consultation procedure on the amendment to the legal bases, which was drafted by the Federal Chancellery. A consultation procedure for the redesign of the e-voting trials was initiated in April 2021 by the Federal Council. 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 [5] defining the foundations for assessing the compliance of electronic voting systems with the draft OEV and its annex [6], as per chapter 26 of the annex of the draft OEV, and for obtaining recommendations for improvements.

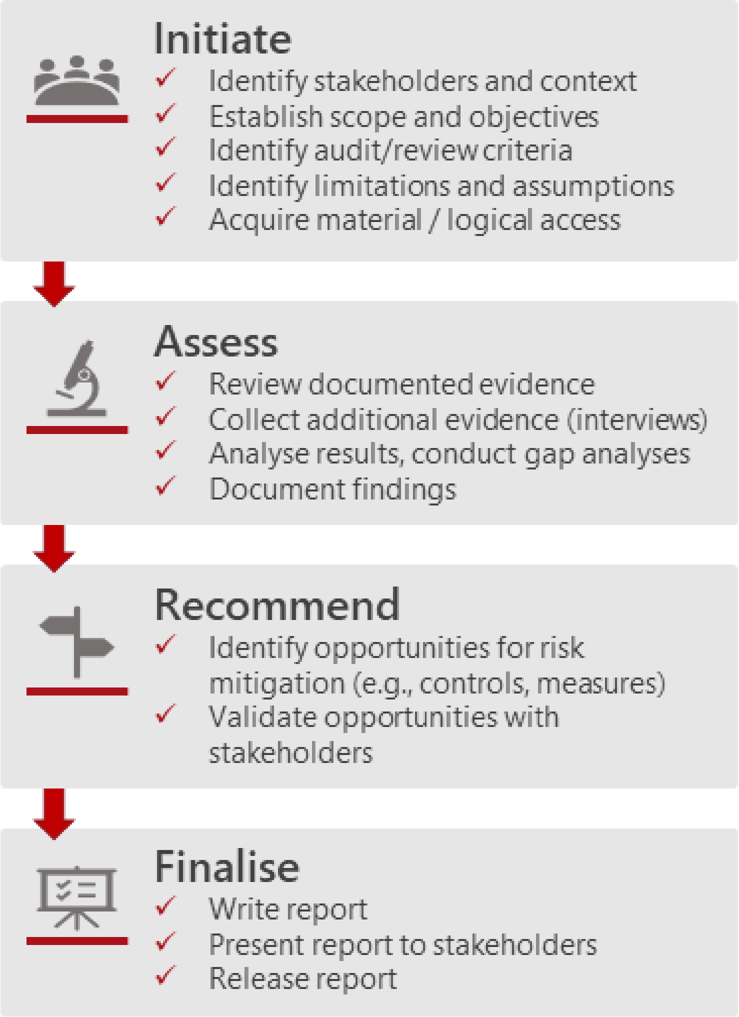
6. SCRT was mandated by the Federal Chancellery to assess the compliance of the Swiss Post's revamped e-voting system against some of the requirements of the draft OEV. The present report focusses on the examination of the perimeter defined as follows in the

audit concept: *Scope 3: Infrastructure and operation, b) Assess the infrastructure and organisational measures of the system provider*.

2 Methodology

2.1 Process

8. The examination was based on SCRT's information systems audit methodology. The process specifies four-phases, which are depicted in the figure below:



Initiate
- ✓ Identify stakeholders and context
- ✓ Establish scope and objectives
- ✓ Identify audit/review criteria
- ✓ Identify limitations and assumptions
- ✓ Acquire material / logical access

Assess
- ✓ Review documented evidence
- ✓ Collect additional evidence (interviews)
- ✓ Analyse results, conduct gap analyses
- ✓ Document findings

Recommend
- ✓ Identify opportunities for risk mitigation (e.g., controls, measures)
- ✓ Validate opportunities with stakeholders

Finalise
- ✓ Write report
- ✓ Present report to stakeholders
- ✓ Release report

Figure 1 - Process

2.2 Collection of evidence

9. 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.

10. Part of the examination included reviewing documents classified as confidential by Swiss Post and thus not released to the public. Motives for not disclosing these documents to the public included either or both the a) preservation of the confidentiality of business processes deployed at the organisation level and which may confer Swiss Post a competitive advantage on other actors, and b) the preservation of confidentiality of

operational data (e.g., risk control, infrastructure operations, etc.). Swiss Post confirmed to us that these documents remain accessible to the cantons.

11. At the beginning of the examination, the examiners were provided with an internal document mapping each Federal Chancellery requirement with its corresponding documented evidence [7]

2.3 Findings

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

2.4 Classification of findings

13. 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.

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

2.5 Relevance of the assessment criteria

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

2.6 Assumptions

2.6.1 Trustworthiness of statements

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

2.6.2 Enforcement of security measures

17. The examiners assume that the security measures described in the documents provided as evidence in the context of the present examination are implemented and are effective.

No observation of the actual implementation of the OEV’s requirements within the e-voting system was carried out to verify the accuracy of the statements made in the security documents.

3 Examination criteria

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

Cryptographic protocol: individual verifiability

Key	Requirement
2.5	The voter is given a proof in accordance with Article 5 paragraph 2 in conjunction with Article 6 letters a and b to confirm that the attacker » has not 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.

Table 1 - E-voting requirements: Requirements for the cryptographic protocol: individual verifiability

Trustworthy components in accordance with Number 2 and 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	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.
3.13	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).
3.14	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

Key	Requirement
	unnoticed. In addition to the requirements set out in Number 3, the following requirements apply in this respect: » If a person has physical or logical access to a control component, that person may not have access to any other control component. » The hardware, the operating systems and the monitoring systems for the control components should be distinct from each other. » The control components should be connected to different networks. » A control component must take the form of a physical device. Virtualisation across multiple physical devices is not permitted.
3.15	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.
3.16	Trustworthy components must perform only the intended operations.
3.18	All procedures for dealing with trustworthy components must be documented in writing and in a manner that is easily understood by the persons concerned.
3.19	Any access to and use of a trusted component or data carrier containing critical data must be logged.

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

Information and instructions

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

Table 3 - E-voting requirements: Information and instructions

Tallying votes in the electronic ballot box

Key	Requirement
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 4 - 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.
12.9	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 5 - E-voting requirements: Confidential data

Threats

Key	Requirement
13.1	The threats listed in Numbers 13.3-13.39 are of a general nature and form a minimum basis. They relate to the security objectives and must be taken into account when identifying risks. Depending on the vulnerabilities of the system identified, when the various bodies carry out their risk assessments, the risks are to be specified and considered based on the actual circumstances and depending on the specific threat.
13.2	The following are considered to be potential threats: » inadvertent or intended electronic or physical threats from internal or external actors; » threats resulting from a malfunction of the system or system-supporting elements

Table 6 - E-voting requirements: Threats

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

Key	Requirement
14.1	An infrastructure monitoring system detects incidents that could endanger the security or the availability of the system and alerts the responsible personnel. The personnel deal with incidents according to a predetermined procedure. Crisis scenarios and rescue plans serve as guidelines (and include a plan that guarantees that voting-related activities can continue) and are applied as required. Errors in the registration of votes in the control components and in the ballot box must be detected. Further information relating to the error must be available in order to identify and eliminate the cause. Any incidents detected must be reported to the body responsible at cantonal level.

14.2	Records are created on the infrastructure whose recording, transmission and storage are resistant to manipulation (system logs). The records are consistent with each other and allow the relevant events to be traced when investigating suspected manipulation or errors. They serve as evidence of the complete, unfalsified and exclusive tallying of votes cast in conformity with the system, of compliance with voting secrecy and of the absence of premature results. The content of the records covers at least the following events: » start and end of the audit, identification and authentication processes; » start, restart and end of the voting or election phase; » start of the tallying with the determination of the results; » conduct and results of any self-tests.
14.3	The monitoring and recording of system logs are subject to a continuous improvement process. The improvement process involves an open dialogue between those involved and a regular and objective assessment of the effectiveness of the instruments and processes used. The results of these evaluations will be taken into account
14.4	The monitoring and recording of system logs in no way detracts from the effectiveness of the measures taken to 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.
14.10	The parts of the voting system that are accessible from the internet must be regularly updated in a predetermined and documented process in order to eliminate weaknesses that have become apparent
14.11	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 7 - 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 secret and confidential 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 secret and confidential 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[1] 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 8 - 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 origin).
16.3	Electronic voting is clearly separated from all other applications.

Table 9 - 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	An authorisation process must be set up for information processing facilities in the infrastructure.
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 10 - E-voting requirements: Organisation of information security

Management of non-material and material resources

Key	Requirement

[1] SR **943.03**

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 11 - 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 12 - 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 13 - E-voting requirements: Physical and environment security

Management of communication and operations

Key	Requirement
22.1	Obligations and areas of responsibility must 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 and the security of network services

Table 14 - 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 entry and 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 abuse by third parties.

Table 15 - E-voting requirements: Allocation, administration and withdrawal of access and admission authorisations

Development and maintenance of information systems

Key	Requirement
24.2.1	An operating manual is created that includes the following for each user role:

	» 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	The preparation process describes all the steps necessary for: » 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	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: » 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.
24.3.4	A reliable and verifiable deployment with appropriate security measures must be carried out. This is to ensure that: 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. The deployment allows a chain of proofs to be created for the verification of the software and includes in particular: » 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	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
24.3.6	The chain of evidence of reliable and verifiable compilation and deployment is made publicly available
24.4.1	Processes are defined for the correction of flaws. The processes include: » documentation of specific aspects, in particular with regard to the traceability of flaws for all versions of the software, and of the methods used to ensure that system users have information on flaws, corrections and possible corrective actions; » the obligation to describe the nature and impact of all security flaws, information on the status of work to find a solution and the corrective measures adopted; » a description of how system users can make reports and enquiries about suspected flaws in the software known to the software developers; » a procedure requiring a timely response and automatic dispatch of security flaw reports and appropriate corrective actions to registered system users who may be affected by the flaw.
24.4.2	A process is defined for handling reported flaws. This process ensures that all reported and confirmed flaws are corrected and that the procedures for correction are communicated to system users. It provides for arrangements to ensure that the correction of security flaws does not give rise to new security flaws.
24.4.3	Policies must be defined for the reporting and correction of flaws. These include: » 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 16 - E-voting requirements: Allocation, administration and withdrawal of access and admission authorisations

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 17 - E-voting requirements: Operation

4 Examination results

7. 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	The voter is given a proof in accordance with Article 5 paragraph 2 in conjunction with Article 6 letters a and b to confirm that the attacker » has not 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	Assuming that the cryptographic protocol implemented by the e-voting system enforces the expected properties of individual verifiability and complete verifiability and is not likely to be defeated by an adversary (the proof of which not being part of the present assessment scope), the ability for a voter to ascertain whether his or her vote has been manipulated or intercepted on the user device or during transmission (Article 5 paragraph 2 alinea a.) is provided through the following means: » Authentication of the voting person and initiation of the voting process thanks to a Start Voting Key; » Validation of the voting option thanks to the receipt of a Choice Return Code to be compared with the ones for each selected voting option; » Comparison of the Choice Return Codes with the ones printed on the individual voting card, casting of the vote thanks to the Ballot Casting Key; » Validation of the vote cast thanks to the Vote Cast Return Code. These means comply with the requirements listed in the Article 5 paragraph 2 alinea b.: *Proof that the trustworthy part of the system has registered the vote as it was entered by the person voting on the user device as being in conformity with the system is obtained*. Confirmation of correct registration is provided for each partial vote. A person who has not cast a vote electronically may request proof, after the electronic ballot is closed and within the statutory appeal deadlines, that the trustworthy part of the system has not registered any vote. To do so, the person must contact the canton, that is able to verify in the logs received from the Post, whether the codes corresponding to the voter's card have been generated and have been used. The procedure is, however, informal.

	The soundness of the proof that a person's vote has not been manipulated or intercepted is actually not based exclusively on the trustworthiness of: » The trustworthy part of the system; » The procedure for generating and printing the voting papers. Indeed, the soundness of the proof also bases on the trustworthiness of the procedure for distributing the printed voting material (which is considered trustworthy, as specified in Article 2.10.2). It is neither the case for the proof that no attacker has cast a vote on the behalf of the person, as its soundness relies on the trustworthiness of the procedure previously depicted, which requires the voter to request information from the canton.
Evidence	» Protocol of the Swiss Post Voting System v0.9.11 » SwissPost Voting System architecture document v1.0 » Swiss Post Voting System Specification v.0.9.7
Result	Partially fail
Finding	The soundness of the proof in accordance with Article 5 paragraph 2 is based on the trustworthiness of the procedure for distributing the voting papers and the trustworthiness of the procedure for requesting information for the cantons. Therefore, the examiners cannot confirm the exclusive nature of the requirements set in Article 6 letters a and b.
Relevance	It seems to the examiners that this requirement does not relate to the current scope of examination. The result (*partially fail*) corresponds to a non-compliance with the requirement, which is however not related to any implementation failure by the Post in the examiners' view, but rather to an incomplete enumeration in the OEV of the conditions, necessary to achieve a sound proof that a vote has not been manipulated or intercepted.

Table 18 – Examination results: OEV paragraph 2.5

Requirements for trustworthy components in accordance with Number 2 and 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	Components mentioned under Number 3.1 include:

	» The set-up component, which runs in a controlled, offline environment of the cantons; » At least one control component which contains part of the key for decrypting the vote. This component is the mixing control component, which shuffles (and re-encrypts) the previous control component’s ciphertexts and performs the final decryption. It runs also in a controlled offline environment of the cantons. The component mentioned under Number 3.3 is the technical aid. This term is mentioned in the Swiss Post Voting System Specification v.0.9.7 document. It is the verifier software used by the auditor/verifier who checks an election event. It runs in a controlled, offline environment of the cantons. The print component runs on the Secure Data Manager, which is operated in a controlled, offline environment of the cantons. The Post only operates the online control components' functionality, which is not involved in the decryption of votes.
Evidence	» SwissPost Voting System architecture document v1.0 » Swiss Post Voting System Specification v.0.9.7
Result	Pass
Finding	N/A
Relevance	N/A

Table 19 – Examination results: OEV paragraph 3.5

Key	3.6
Requirement	Trustworthy components (set-up components, print components, auditors' technical aids and control components) must be set up, updated, configured and secured in an observable process.
Observation	The control components are the only trustworthy components under the sole responsibility of the Post. When performing changes to the control components, the Post implements the notion of “observable process” by: » Enforcing the four-eyes principle when accessing the control components (which involves persons from different teams); » Thoroughly documenting the operations performed. The said operations include the following tasks performed on control components: » Physical installation; » Installation of their operating system; » Change of root passwords; » Change of Integrated Lights-Out (ILO) password.

	Other changes to components (e.g., emergency changes, changes following an incident, etc.) are handled following the formal and mature Post's change management process. The installation procedure of the e-voting software on the control component is currently not formalised.
Evidence	» 4-eye principle Access » E-Voting 4-Augen-Prinzip Kontrollkomponente Einbau Prozess » E-Voting 4-Augen-Prinzip Kontrollkomponente Einbau Protokoll » E-Voting Kontrollkomponente Inbetriebnahme Protokoll » E-Voting Hardening Guidelines » E-Voting Installation Anleitung » 2021-09-21_Protokoll-CC_Nr_-v2-20210921_113641.pdf » Post Change Management » E-Voting Change Management Konzept
Result	Partially fail
Finding	The installation procedure of the e-voting software on the control component is currently not formalised. Therefore, the examiners cannot ascertain that it is performed in an observable manner.
Relevance	The concepts of "set-up components", "print components" and "technical aid" are not defined in the OEV, which prevents an objective interpretation of the examination criterion.

Table 20 – 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	The Post has developed a procedure to ensure that the pieces of software made available for installation on the e-voting components managed by the cantons be the correct and unaltered versions. The pieces of software are downloaded by the cantons from a Gitlab repository. A hash of each binary is provided on the collaboration platform between the Post and the cantons to enable the verification of their integrity via a different communication channel. The procedure concerns all software run on the trustworthy components, including tools used to manage ballots and the Secure Data Manager (SDM), the latter being foreseen to be integrated to the Post's "trusted build concept" at a later stage. The trusted build concept provides a hash of the e-voting system software artefacts so that it can be verified that the software installed by the Post is the compiled version of the code stored on the Post's source code repository.

Evidence	» Trusted Build of the Swiss Post Voting System » E-Voting Checkliste » E-Voting Collaboration Platform » E-Voting Hash Überprüfung Anleitung » Recommendation safety measures (SDM hardening guidelines)
Result	Pass
Finding	N/A
Relevance	N/A

Table 21 – Examination results: OEV paragraph 3.7

Key	3.8
Requirement	The timing for updating all software of trustworthy components must be such that the expected benefits outweigh the potential hazards.
Observation	Components' updates (at infrastructure, middleware and application level) are handled following the formal and mature Post's change management process. To avoid potential hazards, two change phases have been defined and apply to the e-voting system's components (green and red). The green phase corresponds to a maintenance window of 2-3 weeks that takes place once per quarter and starts after a ballot. The red phase corresponds to a freeze period. During a red period, it is possible to proceed to emergency changes only. The possible cases are depicted in a specific document (*E-Voting Ereigniskommunikationsmatrix*). In particular, when a vulnerability affecting a component is identified, the Post security team takes a risk-based decision.
Evidence	» E-Voting Wartung Konzept » E-Voting Checkliste » E-Voting Ereignisentscheidungsmatrix » Post Change Management » E-Voting Change Management Konzept
Result	Pass
Finding	N/A
Relevance	N/A

Table 22 – Examination results: OEV paragraph 3.8

Key	3.10
Requirement	Trustworthy components may not be connected to the internet when installing or updating software.

Observation	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. No update is performed on control components. They are always reinstalled from scratch, and the process is performed offline.
Evidence	» E-Voting Layer 4 Konzept » Post HB Network Security Architecture » Post VOR-Internet Outbound Prozess
Result	Pass
Finding	N/A
Relevance	N/A

Table 23 – Examination results: OEV paragraph 3.10

Key	3.13
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	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. Access to the control components is performed by submitting an access request to a dedicated team (token team), which itself has no access to the network zones where the control components reside. All logical actions on control components are subject to a formal report signed by the parties involved. Teams with logical access to the control components do not have physical access. Only the infrastructure team is allowed to access the components physically, based on a formal change request and while being accompanied. All physical actions on control components are subject to a formal report signed by the parties involved. The Post's employees are not involved in the management of data carriers, which is the responsibility of the cantons.
Evidence	» 4-eye principle Access » E-Voting Monitoring Konzept » E-Voting Physischer Zutritt Konzept » Post RZ Richtlinien

	» Operational guide for e-voting » Operation whitepaper of the Swiss Post voting system » E-Voting Protokoll Systemzugriffe
Result	Pass
Finding	N/A
Relevance	The notion of data carrier should be defined formally in the context of the e-voting system

Table 24 – Examination results: OEV paragraph 3.13

Key	3.14
Requirement	Success in gaining unauthorised access to a control component should not as far as possible give any advantage in an attempt to access another control component unnoticed. In addition to the requirements set out in Number 3, the following requirements apply in this respect: » If a person has physical or logical access to a control component, that person may not have access to any other control component. » The hardware, the operating systems and the monitoring systems for the control components should be distinct from each other. » The control components should be connected to different networks. » A control component must take the form of a physical device. Virtualisation across multiple physical devices is not permitted.
Observation	Segregation of duties between the Post's operational teams (CC1, CC2, CC3, CC4) enforces the requirement: "If a person has physical or logical access to a control component, that person may not have access to any other control component." Each control component runs on dedicated physical hardware with distinct operating system and is operated in a dedicated network. Access to control components' network is disabled by default and must be explicitly granted, based on a formal access request. From a physical point of view, each control component runs in a dedicated rack located in the most secure zone of the datacentres' provider (Postfinance). The monitoring systems for the control components include Grafana (general health of the systems) and the Splunk security information and event management (SIEM) platform (focus on security events), which collects access logs and host intrusion detection system (HIDS) logs. Those monitoring tools are common to the whole Post's infrastructure. The physical security team members have access to all control components.
Evidence	» 4-eye principle Access » Post's ISO 27001 certificate » Post ISO 27001 Statement of Applicability

	» Swiss Post Cyber Tool Map » E-Voting Layer 4 Konzept » Whitepaper Infrastructure of the Swiss Post Voting System » Post RZ Richtlinien » Physical Access Data Center E-Voting Infrastructure concept » Operation whitepaper of the Swiss Post voting system » 2021-09-21_Protokoll-physischer-Einbau-CC_Nr_-v2-20210921_112152
Result	Partially fail
Finding	The monitoring systems for the control components are not distinct from each other. The Post's datacentre service team has the keys for all control components' racks.
Relevance	N/A

Table 25 – Examination results: OEV paragraph 3.14

Key	3.15
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	Any logical action performed on a control component is monitored, recorded and corresponding alerts are sent to a dedicated team (Storage Team). After each ballot, local access logs are reconciled with the records of the team granting accesses (token team) to ensure consistency. A file integrity verification tool (Samhain) detects modifications of system files. 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. The rooms where the control components are physically hosted are subject to physical access control and video surveillance. The Post applies the following measures to ensure the trustworthiness of its employees: » 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); » Signature by the personnel of non-disclosure agreement (as part of the general Post HR process and e-voting-specific).

Evidence	» E-Voting Samhain Anleitung » E-Voting Monitoring Konzept » Post RZ Richtlinien » E-Voting NDA » Post Anstellung Prozess » Operation whitepaper of the Swiss Post voting system » Physical Access Data Center E-Voting Infrastructure concept » Funktionsweisung Sicherheitsüberprüfung von Mitarbeitenden - Die Schweizerische Post AG » TICK-Stack Übersicht » Geheimhaltungsvereinbarung im Zusammenhang mit dem Projekt/Vertragsverhältnis: E-Voting der Post
Result	Pass
Finding	N/A
Relevance	N/A

Table 26 – Examination results: OEV paragraph 3.15

Key	3.16
Requirement	Trustworthy components must perform only the intended operations.
Observation	This requirement is enforced through hardening measures on control components. The vulnerability management process applied to the control components may also be invoked as a complementary measure to prevent unauthorised actions on the control components by leveraging some vulnerabilities. Finally, penetration testing performed before each ballot provides additional assurance regarding the reliability of the control components. The Oracle database hardening guide transmitted to the examiners refers to v.11gR2 of the product.
Evidence	» HB_Hardening_V0103 » E-Voting Hardening Guidelines » E-Voting Kontrollkomponente Betrieb Handbuch » PR_Sicherheitsluecken_proaktiv_bearbeiten_V0308 » E-Voting Datenbank Konzept » Konzept Hardening Oracle Datenbanken
Result	Partially fail
Finding	The current Oracle database hardening reference guide is a rather old document (2014) that covers an older version (i.e., v.11gR2) of the product than the one supporting the e-voting system. It may therefore not be adapted to the present context.

Relevance	N/A

Table 27 – Examination results: OEV paragraph 3.16

Key	3.18
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	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. Quality controls are performed once a year.
Evidence	» 4-eye principle Access » E-Voting Kontrollkomponente Betrieb Handbuch
Result	Pass
Finding	N/A
Relevance	N/A

Table 28 – Examination results: OEV paragraph 3.18

Key	3.19
Requirement	Any access to and use of a trusted component or data carrier containing critical data must be logged.
Observation	Every access and action performed on a control component is subject to a formal access request and report. Hardening measures applied on the control components include the activation of local logging functionalities. Accesses performed on control components trigger an alarm which is sent to the corresponding CC team. After each ballot, local access logs are reconciled with the records of the team granting accesses (token team) to ensure consistency.
Evidence	» 4-eye principle Access » E-Voting Protokoll Systemzugriffe » E-Voting Überwachung und Alarming Konzept » E-Voting Monitoring Konzept
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 29 – Examination results: OEV paragraph 3.19

Information and instructions

Key	8.12
Requirement	Known flaws and the need for action associated with them are communicated transparently.
Observation	The Post maintains a section related to known issues on the public Gitlab instance where the source code of the e-voting system is published.
Evidence	https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/issues
Result	Pass
Finding	N/A
Relevance	N/A

Table 30 – Examination results: OEV paragraph 8.12

Tallying votes in the electronic ballot box

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 auditors to check it.
Observation	The Post is not involved either in the decryption process or in the transmission of the result of the ballot, which are performed by the cantons. It provides the secure logs before the decryption. At the infrastructure level, the Post has defined two change phases for e-voting (red and green). When a ballot takes place, change management enters in a red phase, where changes are frozen by default. The process allows for emergency changes during the red period, e.g., in case of incident. A four-eyes principle applies for the management of the components (reverse proxy, front-end & back-end servers, databases, control components). All accesses performed are logged.
Evidence	» Operational guide for e-voting

	» E-Voting Change Management Konzept » People and Role » Whitepaper Infrastructure of the Swiss Post Voting System » 4-eye principle Access » E-Voting Protokoll Systemzugriffe
Result	Pass
Finding	N/A
Relevance	N/A

Table 31 – 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	One of the security objectives of the e-voting system is to provide vote secrecy (i.e. the property that preserves the privacy of the voter). It is guaranteed by the cryptographic protocol implemented by the system (the reliability of which being out of the present examination scope). On the infrastructure side, TLS v1.3 provides an additional layer of protection of the communications between the voter's browser and the voting server (server authentication and communication confidentiality). One plausible scenario to allow a connection to be made between the identity of persons voting and the votes they have cast would be to trigger the execution of a script in the browser's context to capture the voter's choice (e.g. by exploiting a cross-site scripting attack or modifying the voting portal's webpages). Static and dynamic tests (public review of the e-voting system's source code, bug bounty program, penetration testing) have not revealed any way to defeat this property as of today.
Evidence	» Protocol of the Swiss Post Voting System v0.9.11 » SwissPost Voting System architecture document v1.0 » Swiss Post Voting System Specification v.0.9.7 » https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/issues
Result	Pass
Finding	N/A
Relevance	N/A

Table 32 – 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	One of the security objectives of the e-voting system is to provide vote secrecy (i.e. the property that preserves the privacy of the voter). It is guaranteed by the cryptographic protocol implemented by the system (the reliability of which being out of the present examination scope). Static and dynamic tests (public review of the e-voting system's source code, bug bounty programs) have not revealed any way to defeat this property as of today.
Evidence	» Protocol of the Swiss Post Voting System v0.9.11 » SwissPost Voting System architecture document v1.0 » Swiss Post Voting System Specification v.0.9.7
Result	Pass
Finding	N/A
Relevance	N/A

Table 33 – Examination results: OEV paragraph 12.2

Key	12.9
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	The Post maintains a documented process concerning the destruction of all electronic data created as part of a ballot:
	» Election results (stored after the application of the cryptographic protocol which ensures voting secrecy), including the data stored on control components;
	» E-voting application logs;
	» Control components logs;
	» System logs.
	It encompasses the data stored on the following components:
	» Reverse proxy;
	» Splunk Security Information and Event System (SIEM);
	» Databases;
	» Application servers;
	» Firewalls;
	» Backups media.

	The destruction of the data occurs upon the cantons' instructions, once the legal recourse time within the election process has expired. The retention time for the e-voting data is set to 180 days, which requires backups to be created. Indeed, the standard retention period for the SIEM, firewall and proxy components is one year, and fourteen days for the databases. Those backups are encrypted according to the Post's formal procedure to prevent from unauthorised access to the saved data.
Evidence	» Data destruction concept-v6-20211019_132043 » E-Voting Urnengang Nachbearbeitung Prozess » Operational guide for e-voting
Result	Pass
Finding	N/A
Relevance	N/A

Table 34 – Examination results: OEV paragraph 12.9

Threats

Key	13.1
Requirement	The threats listed in Numbers 13.3-13.39 are of a general nature and form a minimum basis. They relate to the security objectives and must be taken into account when identifying risks. Depending on the vulnerabilities of the system identified, when the various bodies carry out their risk assessments, the risks are to be specified and considered based on the actual circumstances and depending on the specific threat.
Observation	The Post has issued an Information Security and Data Privacy concept (ISDP concept) that takes into account the said threats. At the time of the review, the document is not entirely formalised. As an example, DNSSEC is not mentioned as a countermeasure for DNS poisoning, although DNSSEC is implemented. A comprehensive analysis of the document has not been performed, as it was only made available to the examiners for a limited period during an onsite visit. Risks are evaluated according to the Post general process for information security risk management, which uses a method based on the Credible Worst scenario.
Evidence	» E-voting ISDS Konzept » Funktionsweisung Risikomanagement Informationssicherheit
Result	Partially fail

Finding	The ISDP concept related to the e-voting system, which serves as a basis for the evaluation of the risks pertaining to the system, is not finalised at this stage. The examiners note that the Post only considers the threats listed in Numbers 13.3-13.39 in the existing document whereas they should be considered as a minimum basis. For instance, threat scenarios involving vandalism or sabotage on physical components of the e-voting system are not considered, nor accidental availability issues / information disclosure resulting from a bad manipulation by an employee.
Relevance	N/A

Table 35 – Examination results: OEV paragraph 13.1

<table>
<tr><td>Key</td><td>13.2</td></tr>
<tr><td>Requirement</td><td>The following are considered to be potential threats:
» inadvertent or intended electronic or physical threats from internal or external actors;
» threats resulting from a malfunction of the system or system-supporting elements
<table>
<tr><th></th><th>Description</th><th>Security objective concerned (in accordance with Art. 4 para. 3)</th></tr>
<tr><td>13.3</td><td>Malware changes the vote on the user device.</td><td>Accuracy of the result</td></tr>
<tr><td>13.4</td><td>An external attacker redirects the vote using domain name server spoofing (DNS spoofing)[2].</td><td>Accuracy of the result</td></tr>
<tr><td>13.5</td><td>An external attacker changes vote using the man-in-the-middle (MITM) technique[3].</td><td>Accuracy of the result</td></tr>
<tr><td>13.6</td><td>An external attacker sends a maliciously altered ballot paper using MITM.</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 the votes.</td><td>Accuracy of the result</td></tr>
</table></td></tr>
</table>

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

[3] The attacker in a man-in-the-middle attack. This is a type of attack used in computer networks. The attacker is posititioned 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.

13.9	An internal attacker inserts votes.	Accuracy of the result
13.10	A hostile organisation infiltrates the system with the aim of falsifying the result.	Accuracy of the result
13.11	An internal attacker copies voting papers and uses them.	Accuracy of the result
13.12	An external attacker uses social engineering techniques to distract the person voting from following the security measures (individual verifiability).	Accuracy of the result
13.13	An external attacker infiltrates the canton's infrastructure electronically, physically or by means of social engineering and extracts security-relevant data while the parameters of the ballot are being set.	Accuracy of the result
13.14	An external attacker infiltrates the printing office's infrastructure electronically, physically or by means of social engineering and extracts the codes of the polling cards.	Accuracy of the result
13.15	An external attacker infiltrates the postal service's infrastructure electronically, physically or by means of social engineering and steals polling cards.	Accuracy of the result
13.16	An error occurs in the individual verifiability.	Accuracy of the result
13.17	An error occurs in the universal verifiability.	Accuracy of the result
13.18	An error occurs in an auditor's technical aid.	Accuracy of the result
13.19	A backdoor[4] is introduced into the system via a software dependency and is exploited by an external attacker to access the system.	Accuracy of the result, preservation of voting secrecy and exclusion of premature results, accessibility and operability of the voting system, protection of information intended for voters from manipulation,

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

		prevention of improper use of evidence of voting behaviour
13.20	Malware on the user device sends the vote to a hostile organisation.	Preservation of voting secrecy and exclusion of premature results
13.21	The vote is redirected using DNS spoofing.	Preservation of voting secrecy and exclusion of premature results
13.22	An external attacker reads a vote using MITM.	Preservation of voting secrecy and exclusion of premature results
13.23	An internal attacker uses the key and decrypts non-anonymous votes.	Preservation of voting secrecy and exclusion of premature results
13.24	While checking the accuracy of the processing and tallying, voting secrecy is breached.	Preservation of voting secrecy and exclusion of premature results
13.25	An internal attacker reads the votes at an early stage without having to decrypt the votes.	Preservation of voting secrecy and exclusion of premature results
13.26	A hostile organisation infiltrates the system with the aim of breaching voting secrecy or obtaining premature results.	Preservation of voting secrecy and exclusion of premature results
13.27	An error in the encryption process renders it inoperable or reduces its effectiveness.	Preservation of voting secrecy and exclusion of premature results
13.28	Malware on the user device makes voting impossible.	Accessibility and operability of the voting system
13.29	A hostile organisation carries out a denial-of-service (DOS)[5] attack.	Accessibility and operability of the voting system
13.30	An internal attacker carries out an incorrect configuration; it does not get to the tallying.	Accessibility and operability of the voting system
13.31	An internal attacker falsifies the cryptographic proofs of universal verifiability.	Accessibility and operability of the voting system
13.32	A technical error in the system causes the system to be unavailable at the time of the count.	Accessibility and operability of the voting system

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

<table>
<tr><td></td><td>13.33</td><td>One of the auditors' technical aids does not work at the time of tallying.</td><td>Accessibility and operability of the voting system</td></tr>
<tr><td></td><td>13.34</td><td>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.</td><td>Accessibility and operability of the voting system, protection of information intended for voters from manipulation, prevention of improper use of evidence of voting behaviour</td></tr>
<tr><td></td><td>13.35</td><td>An internal attacker steals voters' address data.</td><td>Protection of personal information relating to voters</td></tr>
<tr><td></td><td>13.36</td><td>Malware influences voters’ opinions.</td><td>Protection of information intended for voters from manipulation</td></tr>
<tr><td></td><td>13.37</td><td>An internal attacker manipulates the information website or voting portal and thereby deceives voters.</td><td>Protection of information intended for voters from manipulation</td></tr>
<tr><td></td><td>13.38</td><td>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.</td><td>Prevention of improper use of evidence of voting behaviour</td></tr>
<tr><td></td><td>13.39</td><td>An external attacker tells voters whether and how they have to vote and demands evidence that they have followed the instructions.</td><td>Prevention of improper use of evidence of voting behaviour</td></tr>
<tr><td>Observation</td><td colspan="3">The listed threats have been considered in the Information Security and Data Privacy concept elaborated by the Post.</td></tr>
<tr><td>Evidence</td><td colspan="3">E-voting ISDS Konzept</td></tr>
<tr><td>Result</td><td colspan="3">Pass</td></tr>
<tr><td>Finding</td><td colspan="3">N/A</td></tr>
<tr><td>Relevance</td><td colspan="3">N/A</td></tr>
</table>

Table 36 – Examination results: OEV paragraph 13.2

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

Key	14.1
Requirement	An infrastructure monitoring system detects incidents that could endanger the security or the availability of the system and alerts the responsible personnel. The personnel deal with incidents according to a predetermined procedure. Crisis scenarios and rescue plans serve as guidelines (and include a plan that guarantees that voting-related activities can continue) and are applied as required. Errors in the registration of votes in the control components and in the ballot box must be detected. Further information relating to the error must be available to identify and eliminate the cause. Any incidents detected must be reported to the body responsible at cantonal level.
Observation	The Post's general Security Information and Event System (SIEM) collects logs related to the e-voting system components. Security events are handled following the Post's general incident response management process. Some specific e-voting events are collected. In particular, root activity is monitored. A set of predetermined incident scenarii has been defined to allow an optimal treatment in case of occurrence. They include adequate coordination with the cantonal authorities. In case of error in the registration of votes, the return codes on the control components would differ and records would not be written. However, no alarm is currently defined for this use case.
Evidence	» Post Incident Response Management Prozess » Indikatoren für IT-sicherheitsrelevante Ereignisse » E-Voting Monitoring Konzept » E-Voting Ereignisentscheidungsmatrix » Handbuch Network Security Architecture » Root Activity Monitoring » Emergency Notfallhandbuch
Result	Partially fail
Finding	No alarm is currently set in case of errors in the registration of votes.
Relevance	The availability property is one of the three axes of information security. Therefore, the phrasing "security or availability" is a pleonasm.

Table 37 – Examination results: OEV paragraph 14.1

Key	14.2
Requirement	Records are created on the infrastructure whose recording, transmission and storage are resistant to manipulation (system logs). The records are consistent with each other and allow the relevant events to be traced when investigating suspected manipulation or errors. They serve as evidence of

	the complete, unfalsified and exclusive tallying of votes cast in conformity with the system, of compliance with voting secrecy and of the absence of premature results. The content of the records covers at least the following events: » start and end of the audit, identification and authentication processes; » start, restart and end of the voting or election phase; » start of the tallying with the determination of the results; » conduct and results of any self-tests.
Observation	The container orchestrator system (Kubernetes) supporting the e-voting system produces extensive logs that are formatted and forwarded to the Post's security information and event system (SIEM). The transmission occurs over TLS, and they cannot be edited in the SIEM, which guarantees their integrity. Logs are time-stamped using a common NTP source and time zone for consistency purpose. The precise nature of the events to be logged is defined at the application level, which is not part of the present evaluation scope.
Evidence	» Swiss Post Voting System Specification v.0.9.7 » Protocol of the Swiss Post Voting System v0.9.11
Result	Pass
Finding	Pass (as far as the aspects related to infrastructure and operation are concerned)
Relevance	N/A

Table 38 – 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	At the end of each ballot, a formal debriefing takes place between the Post and the cantons, where lessons learned are reviewed for continuous improvement purpose. Moreover, if security events are detected, they are managed following the Post's incident detection and response process, which includes a phase of lessons learned.
Evidence	» E-Voting Urnengang Nachbearbeitung Prozess » E-Voting Debriefing Protokoll » E-Voting Urnengang Quality Gate Checkliste

	» Sicherheitsvorfälle bearbeiten (Security Incident Response)
Result	Pass
Finding	N/A
Relevance	N/A

Table 39 – 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	A review of a sample log file containing all the events related to an election event did not reveal any record breaching the voting secrecy principle. The examiners assume that the e-voting application has been designed in a way that the system logs produced do not have a level of verbosity likely to breach the voting secrecy principle (proof of which is not part of the present assessment scope).
Evidence	Sample Splunk log file related to a test election event
Result	Pass
Finding	N/A
Relevance	The notion of “system logs” should be defined formally in the OEV, in order to avoid any confusion between logs produced by the e-voting components and logs produced by the e-voting application (a.k.a., “secure logs”)

Table 40 – 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	The Post has implemented a high-availability concept for the whole e-voting system, based on clusterisation, distant datacentres, triple mirroring and zero data loss for databases. Each control component is also built upon two load balanced nodes hosted in separate datacentres. The Post conducts regular disaster recovery tests to verify the efficiency of the high-availability concept. Additionally, the Post’s general backup procedures apply to the e-voting system.
Evidence	» Whitepaper Infrastructure of the Swiss Post Voting System » Oracle Databases-v9-20211019_131624

	» 2021-09-21 Testprotocol Disaster Recovery » Handbuch Datensicherung
Result	Pass
Finding	N/A
Relevance	N/A

Table 41 – 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	The e-voting system's architecture has been designed to be highly reliable. It bases upon high-availability, fault tolerance and recoverability principles. In particular, voters' keystores and votes are persisted in the voting server's databases, which allows the voter to complete their voting process in case of service interruption. If two out of three databases are not available, votes are not possible (a "sorry page" is displayed).
Evidence	» E-Voting Ereignisentscheidungsmatrix » Prozess Urnengang Durchführen » Post Incident Prozess » Emergency Notfallhandbuch Konzept » E-Voting Notfall Handbuch » SwissPost Voting System architecture document v1.0
Result	Pass
Finding	N/A
Relevance	N/A

Table 42 – Examination results: OEV paragraph 14.6

Key	14.8
Requirement	Infrastructure availability must be checked and recorded at selected intervals.
Observation	The monitoring concept includes monitoring the availability of the e-voting system during a ballot. At the end of the ballot, a report is issued.
Evidence	» E-Voting Monitoring Konzept » E-Voting Change Management Konzept

	» Post Incident management Process
Result	Pass
Finding	N/A
Relevance	N/A

Table 43 – Examination results: OEV paragraph 14.8

Key	14.10
Requirement	The parts of the voting system that are accessible from the internet must be regularly updated in a predetermined and documented process in order to eliminate weaknesses that have become apparent.
Observation	The e-voting system components are subject to the Post's general vulnerability management process. Patches are either deployed on a regular basis during maintenance windows or in an emergency mode for critical vulnerabilities.
Evidence	» Function directive IT baseline protection » Sicherheitslücken proaktiv bearbeiten (Security change / patch management) » Richtlinie Network Security Policy
Result	Pass
Finding	N/A
Relevance	The examiners suggest not to limit this requirement to systems accessible from internet.

Table 44 – Examination results: OEV paragraph 14.10

Key	14.11
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 documents listed here below contain the measures put in place to monitor events such as: » The e-voting system's usage; » The activities of administrators; » The e-voting system's malfunctions. Those documents are reviewed at regular intervals as per the Post quality management process' requirements.
Evidence	» 4-eye principle Access » E-Voting 4-Augen-Prinzip Kontrollkomponente Einbau Prozess » E-Voting 4-Augen-Prinzip Kontrollkomponente Einbau Protokoll

	» E-Voting Monitoring Konzept » E-Voting Zugriffsvalidierung Checkliste
Result	Pass
Finding	N/A
Relevance	N/A

Table 45 – Examination results: OEV paragraph 14.11

Use of cryptographic measures and key management

Key	15.1
Requirement	Electronic certificates must be managed according to the best practices.
Observation	Electronic certificates used in the context of the e-voting system are managed according to the general practices detailed in the Post's certificate policy and certificate practice statement. Some additional best practices are detailed in the Post's policy on cryptography (*Handbuch Kryptographie*). The latter policy requires applications with increased security requirements to implement certificate pinning, which the voting portal and the administration portal do not.
Evidence	» Handbuch Kryptographie » Handbuch Certificate Policy / Certification Practice Statement » E-Voting Passwort Zertifikat Management » E-Voting Zertifikat Management » E-Voting Zertifikat Erneuerung Prozess
Result	Partially fail
Finding	The e-voting system does not implement the requirements of the Post's security policy on cryptography with regards to certificate pinning.
Relevance	N/A

Table 46 – 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 secret and confidential data, including the authorities' identification and authentication data, are kept secret, effective cryptographic measures that correspond to the state of the art must be used.
Observation	The integrity of data records that substantiate the accuracy of the result, and the confidentiality of e-voting is partly addressed through

	cryptographic measures at the application level, which is not in the scope of the present examination. At the infrastructure level, some usages of cryptography contribute to the overall preservation of the e-voting data's integrity and confidentiality, e.g.: » The e-voting system components communicate over TLS v1.3 with mutual authentication. This protects the integrity and confidentiality of the data processed within the e-voting system during transport and ensures that all participating nodes are authenticated to each other. Mutual authentication includes connections to the e-voting administration portal initiated by the cantons; » Administration tasks carried out by the Post's personnel are performed over encrypted channels (e.g. TLS, SSH etc.), and the credentials used to perform those tasks are stored in encrypted password vaults (CyberArc); » Hashes of the JavaScript files served by the voting server's back-end are checked at the reverse proxy level to ensure that the said files have not been manipulated. Implementation of cryptographic measures is performed according to the Post's general security policy on cryptography (*Handbuch Kryptographie*), which provides state-of-the-art instructions regarding the use of algorithms and key lengths (deprecated/valid algorithms, minimum key length, year from which the ley length must be increased and new minimum key length). However, an exhaustive list of the cryptographic security controls implemented within the e-voting system and the link with the threats they mitigate is not formalised.
Evidence	» Handbuch Kryptographie » Infrastructure whitepaper of the Swiss Post voting system » SwissPost Voting System architecture document v1.0 » Certificates and Keys-v13-20211019_131920
Result	Partially fail
Finding	The Post has not formally documented how cryptographic controls implemented within the e-voting system mitigate specific threats at the infrastructure level (e.g. in its ISDS concept or in a threat model).
Relevance	The terms "secret data" and "confidential data" are not defined in the OEV, which prevents an objective interpretation of the requirement.

Table 47 – Examination results: OEV paragraph 15.2

Key	15.3
Requirement	To ensure that secret and confidential 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	At the infrastructure level, some usages of cryptography contribute to the overall preservation of the e-voting data's integrity and confidentiality, e.g.:

	» The e-voting system components communicate over TLS v1.3 with mutual authentication. This protects the integrity and confidentiality of the data processed within the e-voting system during transport and ensures that all participating nodes are authenticated to each other; » Administration tasks carried out by the Post's personnel are performed over encrypted channels (e.g. TLS, SSH etc.), and the credentials used to perform those tasks are stored in encrypted password vaults (CyberArc); » Hashes of the JavaScript files served by the voting server's back-end are checked at the reverse proxy level to ensure that the said files have not been manipulated. Implementation of cryptographic measures is performed according to the Post's general security policy on cryptography (*Handbuch Kryptographie*), which provides instructions regarding the use protocols and key lengths. However, an exhaustive list of the cryptographic security controls implemented within the e-voting system and the link with the threats they mitigate is not formalised. The Post issues recommendations to the cantons regarding encryption on data carriers but does not use such carrier itself.
Evidence	» Handbuch Kryptographie » Infrastructure whitepaper of the Swiss Post voting system » SwissPost Voting System architecture document v1.0
Result	Partially fail
Finding	The Post has not formally documented how cryptographic controls implemented within the e-voting system mitigate specific threats at the infrastructure level (e.g. in its ISDS concept or in a threat model).
Relevance	The terms "secret data" and "confidential data" are not defined in the OEV, which prevents an objective interpretation of the requirement.

Table 48 – Examination results: OEV paragraph 15.3

Key	15.4
Requirement	Basic cryptographic components may only be used if the key lengths and algorithms correspond to the current standards (e.g. NIST, ECRYPT, ESigA). The electronic signature meets the requirements of an advanced electronic signature in accordance with the Federal Act of 18 March 2016 on Electronic Signatures (ESigA)[6]. 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	The length of keys used by cryptographic components operated by the Post is specified in the policy on cryptography (*Handbuch Kryptographie*). The

[6] https://www.fedlex.admin.ch/eli/cc/2016/752/de

	requirements set in the document correspond to current best practices in terms of algorithms and key length. The requirements for an advanced electronic signature, as defined in the EsigA, are as follows: » Be uniquely linked to the holder; » Allow the holder to be identified; » Be created by means that the holder can maintain under its exclusive control; » Be linked to the data to which it relates in such a way that any subsequent change to the data is detectable. The e-voting system uses electronic signature in a way that satisfies those requirements. It is verified by means of a certificate that is sourced from the SwissSign company, which is a recognised supplier of certificate services under the ESigA.
Evidence	» Handbuch Kryptography » Certificates and Keys-v13-20211019_131920 » Handbuch Certificate Policy / Certification Practice Statement » (PKI INT)
Result	Pass
Finding	N/A
Relevance	The notion of “basic cryptographic components” is not defined in the OEV, which prevents an objective interpretation of the requirement.

Table 49 – Examination results: OEV paragraph 15.4

Secure electronic and physical exchange of information

Key	16.1
Requirement	All infrastructure components must be operated in a separate network zone. This network zone must be protected in relation to other networks by an appropriate routing control.
Observation	At the exception of control components, the e-voting system's infrastructure components implement a microservice architecture made of containers (Docker?), whose lifecycle is controlled by the Kubernetes container orchestration platform. The cluster is composed of several worker nodes for each canton. Each worker node is a virtualised machine based on the VMWare technology. 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.

	The access layer to the e-voting system is composed of four dedicated reverse proxies (two per datacentre) running on physical servers. The proxies are hosted in a Post's dedicated DMZ. The other e-voting infrastructure components are hosted in dedicated zones within the Post's internal network, that represent trust boundaries between the individual components. 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. 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). In addition to network filtering, iptables are defined at operating system level for each pod, which forms a second way of filtering communication flows between the e-voting components.
Evidence	» Post HB Network Security Architecture » Infrastructure whitepaper of the Swiss Post voting system » Area-Beschreibung und Platzierungskriterien DCP (Dynamic » Computing Platform)
Result	Pass
Finding	N/A
Relevance	This requirement addresses the filtering of communications between the different components forming the e-voting system (e.g. front-end / back-end / database). However it does not mention any requirements regarding a segregation of environments between the cantons, which should be considered as a mandatory practice (and is implemented).

Table 50 – 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	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. The Post's risk assessment of the e-voting system considers a wide range of attacks. Protection measures are implemented to mitigate the risk of threat

	materialisation to a residual level. They consist of both a common security baseline and countermeasures for e-voting specific threats.
Evidence	» Post's ISO 27001 certificate » Post's ISO 27001 Statement of Applicability » Function directive IT baseline protection » E-voting ISDS Konzept » Swiss Post Cyber tool map
Result	Pass
Finding	N/A
Relevance	N/A

Table 51 – Examination results: OEV paragraph 16.2

Key	16.3
Requirement	Electronic voting is clearly separated from all other applications.
Observation	The observation made for the requirement 16.1 shows how the e-voting system is hosted in dedicated networks. The access layer to the e-voting system is composed of four dedicated reverse proxies (2 per datacentres) running on physical servers. The e-voting infrastructure components which run in a virtualised environment (i.e., all components at the exception of the access layer and the control components) are operated from a dedicated VMWare hypervisor. The e-voting databases run on a dedicated Oracle Database Appliances (ODA) platform.
Evidence	» Infrastructure whitepaper of the Swiss Post voting system » Area-Beschreibung und Platzierungskriterien DCP (Dynamic » Computing Platform)
Result	Pass
Finding	N/A
Relevance	The expressions "electronic voting" and "clearly separated" are too vague to allow an objective interpretation of the requirement. To draw their conclusion, the examiners considered that: » The SIEM infrastructure that collects the e-voting's infrastructure security logs (which is common to the Post's whole environment) is not a component of the "electronic voting"; » The requirement for separation does not imply dedicated maintenance personnel.

Table 52 – Examination results: OEV paragraph 16.3

Organisation of information security

Key	18.1
Requirement	All roles and responsibilities for the operation of the system must be precisely defined, assigned and communicated.
Observation	The *People and roles* document includes a matrix which shows which teams within the Post is in charge of which component of the e-voting system.
Evidence	People and roles
Result	Pass
Finding	N/A
Relevance	N/A

Table 53 – Examination results: OEV paragraph 18.1

Key	18.2
Requirement	An authorisation process must be set up for information processing facilities in the infrastructure.
Observation	The examiners understand that this requirement relates to the authorisation process in case of changes. Change management at the e-voting level follows the Post's general change management process, which bases upon ITIL best practices, and therefore includes an authorisation step. The *E-Voting Change Management Konzept* document details the authorisation workflow, which involves both the IT-Post and the e-voting Change Advisory Boards.
Evidence	» Post change management » E-Voting Change Management Konzept
Result	Pass
Finding	N/A
Relevance	This requirement should be reformulated in order to refer explicitly to changes.

Table 54 – 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	The Post maintains a list of service suppliers providing IT-related and information security related service in relation to e-voting specifically (i.e. with which a contractual relationship exists). The lists references company-to-company non-disclosure agreements signed between the Post and its service providers. Postfinance is not mentioned as the supplier of the e-voting system's datacentres, although some of its employees are allowed access to the datacentres' rooms hosting the e-voting system servers, and therefor represent threat agents to the system. The Post's supplier management process includes a risk assessment based on the criticality of the data that the suppliers process in the context of the service they deliver. Assessments must be reviewed on a yearly basis. No evidence was shown to the examiners that the risk assessment process has taken place for the suppliers listed in the *E-Voting: Liste Verträge* document.
Evidence	» E-Voting: Liste Verträge » Handbuch supplier security management
Result	Fail
Finding	No evidence was shown to the examiners that the Post's standard supplier security management process has been applied to the companies involved in the e-voting supply chain. Moreover, the document shown to the examiners fails to mention some suppliers (e.g. Postfinance, as the datacentres' provider, which contract is managed directly by PostIT).
Relevance	N/A

Table 55 – Examination results: OEV paragraph 18.3

Management of non-material and material resources

Key	19.1
Requirement	All intangible and tangible resources in the sense of the term asset in the standard ISO/IEC 27001, 2013, Information technology - Security techniques - Information security management systems - Requirements, relevant in the context of electronic voting (organisation as a whole, in particular the organisational processes and the information processed in these processes, data carriers, facilities for processing information of the infrastructure and premises of the infrastructure) are recorded in an inventory. A list must be kept of human resources. The inventory and

	human resources list must be kept up to date. Each intangible and tangible resource is assigned a person who takes responsibility for it.
Observation	The 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. The Post's quality management process requires regular reviews of the inventories to ensure they are up-to-date.
Evidence	» Post's CMDB tool (Aixboms) » Adonis tool » IT- Managementsystem tool / E-voting Mitarbeiterliste
Result	Pass
Finding	N/A
Relevance	N/A

Table 56 – Examination results: OEV paragraph 19.1

Key	19.2
Requirement	The acceptable use of non-material and material resources must be defined.
Observation	The Post maintains a general document regarding the acceptable use of assets, which is reviewed regularly. Employees are reminded regularly of the requirements of this document through security awareness campaigns. Employees involved in the e-voting sign both a general and an e-voting-specific non-disclosure agreement.
Evidence	» Funktionsweisung Informationssicherheit am Arbeitsplatz » Geheimhaltungsvereinbarung_Spezifisch-E-Voting-Mitarbeiter
Result	Pass
Finding	N/A
Relevance	N/A

Table 57 – Examination results: OEV paragraph 19.2

Key	19.3
Requirement	Classification guidelines for information must be issued and communicated.

Observation	The Post maintains a general document regarding information classification. It includes classification grades for the confidentiality, integrity, and traceability requirements of information. Classification criteria regarding the availability of information are also provided (i.e. service time, max downtime, max data loss time, specific continuity measures) The analysis of the security needs for e-voting (*Schutzbedarfanalyse*) details the classification grades adopted for the data processed within the e-voting system. The examiners noted that the confidentiality grade mentioned in the *Schutzbedarfanalyse* does not correspond to the taxonomy used in the information classification policy.
Evidence	» Funktionsweisung Klassifierung von Informationen » E-voting Schutzbedarfanalyse
Result	Partially fail
Finding	The confidentiality grade mentioned in the *Schutzbedarfanalyse* document for the data processed within the e-voting system does not correspond to the taxonomy used in the information classification policy.
Relevance	N/A

Table 58 – Examination results: OEV paragraph 19.3

Key	19.4
Requirement	Procedures must be devised for the labelling and handling of information.
Observation	An addendum to the information classification policy details the requirements for labelling and handling information.
Evidence	Factsheet Klassifizierung von Informationen
Result	Pass
Finding	N/A
Relevance	N/A

Table 59 – Examination results: OEV paragraph 19.4

Trustworthiness of human resources

Key	20.1
Requirement	Suitable policies and procedures must be devised and promulgated in order to guarantee the trustworthiness of human resources before, during and after termination of employment or in the case of a change of activity.

Observation	The trustworthiness of the Post's human resources interacting with the e-voting infrastructure is assessed through background checks. Joiners and movers must provide a criminal record extract and sign a declaration stating that they are not involved in criminal or civil proceedings. These controls complement the regular review of the joiners' application file and references. Further checks on employees are possible based of the risks induced by the position. Within the e-voting teams, a certificate from the debt enforcement office is systematically required. Moreover, employees sign both a general and an e-voting-specific non-disclosure agreement, that remains valid after contract termination. Within the e-voting team, the screening process is only performed once, at the beginning of the work relationship. This contradicts the requirement mentioned in the Post's guideline regarding personnel screening, which states that the screening process should be performed every four years for sensitive functions and for managers.
Evidence	» Funktionsweisung Sicherheitsüberprüfung von Mitarbeitenden » «Die Schweizerische Post AG» » Geheimhaltungsvereinbarung » Geheimhaltungsvereinbarung im Zusammenhang mit dem Projekt/Vertragsverhältnis: E-Voting der Post » Auszug_GAV_Geheimhaltung » Auszug_Kaderreglement_Geheimhaltung
Result	Fail
Finding	The screening process on human resources interacting with the e-voting system is only performed once, whereas it should be performed every four years, as specified in the Post's guideline.
Relevance	N/A

Table 60 – Examination results: OEV paragraph 20.1

Key	20.2
Requirement	Human resources managers must accept full responsibility for guaranteeing the trustworthiness of human resources.
Observation	The human resources department is in charge of issuing guidelines regarding the employees' screening process but the examiners did not find any statement that this department assumes the responsibility for guaranteeing the trustworthiness of human resources.
Evidence	Funktionsweisung Sicherheitsüberprüfung von Mitarbeitenden - Die Schweizerische Post AG

Result	Fail
Finding	The examiners did not find any evidence that the Post's human resources department, or any other function assumes the responsibility for guaranteeing the trustworthiness of human resources.
Relevance	N/A

Table 61 – Examination results: OEV paragraph 20.2

Key	20.3
Requirement	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.
Observation	The Post has established an information security awareness concept that pursues the following objectives: » Increase the general awareness of personnel regarding information security through short repetitive messages to maintain the attention of employees; » Enforce the ability to behave in a secure manner through in-depth targeted training; » Ensure the Post's information security function is recognised as the first contact point for information security matters. All employees are subject to e-learning courses that take place every two years. New hires in teams that interact with the e-voting system are subject to specific onboarding sessions that include matters regarding the e-voting infrastructure and its secure operation.
Evidence	» Konzept Security Awareness » Eintritt-Checklist_I351 » Eintritt-Checklist_I353 » Eintritt-Checklist_I354 » Eintritt-Checklist_I356
Result	Pass
Finding	N/A
Relevance	N/A

Table 62 – Examination results: OEV paragraph 20.3

Physical and environment security

Key	21.1

Requirement	The security perimeters of the various premises of the infrastructure are clearly defined.
Observation	The Post’s *HB Sicherheitszonen – Die Schweizerische Post AG* 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
Result	Pass
Finding	N/A
Relevance	N/A

Table 63 – Examination results: OEV paragraph 21.1

Key	21.2
Requirement	For physical entry to these various infrastructure premises, entry controls must be defined, implemented and appropriately checked.
Observation	The Post’s “*KLA-Weisung Zutrittsmanagement - Die Schweizerische Post AG*” document defines which entry controls apply to which security perimeter. The document specifies the responsibilities for the implementation of the entry controls and for their periodic review.
Evidence	KLA-Weisung Zutrittsmanagement - Die Schweizerische Post AG
Result	Pass
Finding	N/A
Relevance	N/A

Table 64 – Examination results: OEV paragraph 21.2

Key	21.3
Requirement	To guarantee the security of devices within and outside the infrastructure premises, appropriate policies and procedures must be defined and compliance therewith monitored and reviewed.
Observation	The devices composing the e-voting system fall 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, whose effectiveness is monitored and reviewed regularly. Remote access to the e-voting system is possible through the corporate VPN from the Post’s laptops only.

	Infrastructure components of the e-voting system are hosted within dedicated server rooms of Postfinance’s datacentres. The said datacentres are Dual Site Level 3 certified against the Trusted Site Infrastructure v4.2 standard. Level 3 certifies the high availability of the datacentres by meeting the following requirements: No single point of failure in the supply systems, increased burglar resistance, safeguarding of supply routes, fire containment and status monitoring. In addition to the physical and environment security measures applied in the context of the Post’s Information Security Management System, e-voting specific measures apply. In particular, the control components are subject to reinforced protection. All interventions requiring physical access to the control components are performed according to the four-eyes principle (one person from the datacentre service team and one person from one of the e-voting teams) and are documented. The control components are stored in dedicated locked racks. Six persons from the datacentre service team in total are granted a one-year renewable access to the keys opening the racks. The keys are stored in a dedicated safe, whose code is itself stored in a Privileged Access Management vault (CyberArc). All staff from the team (sixteen persons) have access to the server rooms themselves in addition to the Postfinance’s infrastructure team, that accesses the rooms autonomously and without the Post being informed. Standard visitor access is granted on an ad hoc basis and is valid for one day. Physical access logs are kept for one year. No alarm is configured to detect potential unauthorised access or access attempts. Quality procedures are defined for the management of datacentres. A review of the installation is performed on a monthly basis and is subject to a report. E-voting devices taken outside the infrastructure include the four notebooks handed over to each canton (i.e. synchronisation computer, configuration computer, decryption computer and verification computer), which run the Secure Data Manager (SDM). Authentication to those notebooks occurs with a smart card reader. Detailed instructions at the attention of the cantons are provided regarding the security precautions to be taken to protect the notebooks against relevant threats.
Evidence	» HB Sicherheitszonen – Die Schweizerische Post AG » KLA-Weisung Zutrittsmanagement - Die Schweizerische Post AG » Physical Access Data Center E-Voting Infrastructure concept » Merkblatt Arbeiten und Verhalten in Rechenzentren von PostFinance AG » Post’s ISO 27001 certificate » Post’s ISO 27001 Statement of Applicability » Function directive IT baseline protection

	» E-Voting: Liste Verträge » https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/Operations/Recommendation_Safety_Measures_SDM.md#catalogue-of-generic-security-measures
Result	Pass
Finding	N/A
Relevance	N/A

Table 65 – Examination results: OEV paragraph 21.3

Key	21.4
Requirement	All data must be processed exclusively in Switzerland, including storage.
Observation	The e-voting system's components operated by the Post are all stored in Postfinance's datacentres located in Bern and Zofingen, Switzerland. However, the source code of the e-voting system is hosted on the Gitlab source code repository in the USA. Third-party libraries used by the e-voting front-end application are downloaded locally.
Evidence	» Infrastructure whitepaper of the Swiss Post voting system » https://gitlab.com/swisspost-evoting
Result	Fail
Finding	The source code of the e-voting system being one of its critical information assets, one cannot state that all data is processed exclusively in Switzerland.
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 66 – Examination results: OEV paragraph 21.4

Management of communication and operations

Key	22.1
Requirement	Obligations and areas of responsibility must 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	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. bad

	manipulation resulting in confidentiality, integrity or availability issues) as well as intentional malicious actions (e.g. fraud attempts, vandalism/sabotage, etc.). The *People and roles* document shows how obligations and 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 (reverse proxy, front-end & back-end servers, databases) limits the risks of frauds. A strict segregation of duties also applies for the management of the control components. People involved in the e-voting operations and communications also follow trainings, which reduces the risk of accidental behaviours. The Post does not use formal risk acceptance criteria to define whether risks are to be considered as residual. Instead, a risk committee including business and technical representatives meets regularly to take such decisions. The current version of the Information Security and Data Privacy concept for the e-voting system does not include threats linked to accidental behaviours by employees.
Evidence	» People and roles » Whitepaper Infrastructure of the Swiss Post Voting System » Schulungskonzept E-Voting » Training concept canton » Handbuch Risikomanagement Informationssicherheit » E-voting ISDS Konzept
Result	Fail
Finding	Although good practices in terms of allocation of obligations and areas of responsibility exist, a comprehensive documentation detailing how those practices mitigate the various types of risks originating from human resources does not seem to be available at this stage.
Relevance	The English version of the OEV contains a typography mistake (“must apportioned”-> “must be apportioned”).

Table 67 – Examination results: OEV paragraph 22.1

Key	22.2
Requirement	Appropriate measures must be taken to protect against malware.
Observation	Protection against malware include a wide range of measures, including user-awareness, end-point protection, management of removable media, rules for software installation, network segregation, patch management, hardening of components, ingress and egress IP communications filtering, content filtering, incident detection and response. All these measures are

	part of the Post Information Security Management System's standard controls. The Linux-based control components run a Security-Enhanced Linux version, a rootkit detection tool, and an intrusion detection system. The Windows-based control component runs the standard Post antivirus software. The Post's Computer Emergency Response Team (CERT) is in charge of handling malware incidents. A malware outbreak at the infrastructure level is one of the crisis scenarios considered in the Post's emergency manual.
Evidence	» Post's ISO 27001 certificate » Post's ISO 27001 Statement of Applicability » Handbuch Network Security Architecture » Handbuch HB hardening » Function directive IT baseline protection » Indikatoren für IT-sicherheitsrelevante Ereignisse
Result	Pass
Finding	N/A
Relevance	N/A

Table 68 – Examination results: OEV paragraph 22.2

Key	22.3
Requirement	A detailed plan for data backup must be prepared and implemented. The data backup must be regularly reviewed to check that it is functioning correctly.
Observation	The backup of the e-voting system's components is performed according to the Post's general backup policy principles. Dedicated documents describe the backup plan for: » The e-voting databases (*E-voting Datenbanken*); » The cluster and management server, the control components (*OVP and control components backup and restore*); The performance of regular restore tests is part of the Post's baseline controls. Evidences are kept on the e-voting wiki.
Evidence	» Function directive IT baseline protection » Handbuch Datensicherung » E-voting Datenbanken » OVP and control components backup and restore
Result	Pass
Finding	N/A

Relevance	For the sake of clarity, the examiners suggest to rephrase the second sentence into "Restore tests of the data backups must be performed regularly".

Table 69 – Examination results: OEV paragraph 22.3

Key	22.4
Requirement	Appropriate measures must be defined and implemented to protect the network and the security of network services
Observation	The Post network and network services, including those supporting the e-voting system, fall 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, whose effectiveness is monitored and reviewed regularly. In its *Network Security Architecture manual*, the Post has defined, in particular, a set of twenty security activities, each of which being broken down into specific implementation requirements. The *Infrastructure whitepaper of the Swiss Post voting system* document details the high-availability properties of the e-voting system, which protect it from breakdowns at network and network service levels.
Evidence	» Post's ISO 27001 certificate » Post's ISO 27001 Statement of Applicability » Swiss Post Cyber Tool Map » Function directive IT baseline protection » Handbuch Network Security Architecture » Infrastructure whitepaper of the Swiss Post voting system
Result	Pass
Finding	N/A
Relevance	The examiners suggest rephrasing this requirement to make it more specific, e.g., by detailing against which threats the network and network services should be protected.

Table 70 – Examination results: OEV paragraph 22.4

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 entry and access rights takes place only with the consent of the body responsible at cantonal level.
Observation	Change management at the e-voting level follows the Post's general change management process, which bases upon ITIL best practices. The Post has defined two change phases for e-voting (red and green). When a ballot takes place, change management enters in a red phase, where changes are frozen by default. The process allows for emergency changes during the red period, e.g., in case of incident. In such a case, the cantons are accountable for the release of the change and therefore consent to it. Physical access requests to the e-voting system's components that may be necessary to handle a change are also dealt with through the change management process.
Evidence	» Post change management » E-Voting Change Management Konzept » Change concept » Physical Access Data Center E-Voting Infrastructure concept
Result	Pass
Finding	N/A
Relevance	The phrasing "subsequent change in entry" should be improved, as it is currently not explicit that this expression refers to physical access rights.

Table 71 – Examination results: OEV paragraph 23.1

Key	23.2
Requirement	Access to infrastructure and software must be regulated and documented in detail on the basis of a risk assessment. In high-risk areas and for all manual operations in connection with the electronic ballot box (e.g. opening the voting channel, closing the voting channel, starting tallying), operations must be conducted by at least two persons. Manual operations in connection with the electronic ballot box (e.g. opening the voting channel, closing the voting channel, starting tallying) must be expressly authenticated.
Observation	Accesses performed by employees and contractors to the e-voting system are subject to the Post's Identity and Access Management policy, which bases upon best practices. In particular, it enforces core principles such as the least privilege rule, the need-to-know principle. Administrative access to the e-voting specific infrastructure (reverse proxy, front-end & back-end servers, databases, control components) is performed following the four-eyes principle.

	High-risk areas and for all manual operations in connection with the electronic ballot box are performed by: » The Administration Board (opening and closing of the voting channel). Two members are required by default, but the threshold can be changed to have only one smartcard to unlock the Administration Board; » The electoral authority (decoding and counting operations). It requires at least two members. Logon to the administration portal requires authentication using a password and a smartcard protected by a PIN. At the time of the examination, the ISDP concept does not document the detailed risks and countermeasures related to accesses to the e-voting system's infrastructure and software.
Evidence	» Handbuch Identity and Access Management (IAM) » Operational guide for e-voting » Infrastructure whitepaper of the Swiss Post voting system » 4-eye principle Access » E-voting ISDS Konzept
Result	Fail
Finding	At the time of the examination, the ISDP concept does not document the detailed risks and countermeasures related to accesses to the e-voting system's infrastructure and software. The examiners cannot conclude that access to infrastructure and software is regulated and documented in detail on the basis of a risk assessment. Moreover, it seems that it is possible to modify the default settings regarding the minimum number of members within the Administration Board. The examiners are therefore not able to ascertain that those manual operations in high-risk areas are conducted by at least two persons.
Relevance	N/A

Table 72 – 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	This requirement may be broken down into two subcategories: » Legitimate changes; » Illegitimate changes performed by internal and external malicious actors. 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.), use of a SIEM combined with incident detection and response, etc. 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.
Evidence	» Post's ISO 27001 certificate » Post's ISO 27001 Statement of Applicability » Post change management » E-Voting Change Management Konzept
Result	Pass
Finding	N/A
Relevance	N/A

Table 73 – Examination results: OEV paragraph 23.3

Key	23.4
Requirement	During the ballot, access to the infrastructure of any nature must be prevented.
Observation	This requirement may be broken down into two subcategories: » Legitimate access; » Illegitimate access performed by malicious actors. 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.), use of a SIEM combined with incident detection and response, etc. With regards to legitimate changes, the Post has defined two change phases for e-voting (red and green). When a ballot takes place, change management enters in a red phase, where changes are frozen by default. The process allows only for emergency changes during the red period, e.g., in case of incident.

Evidence	E-Voting Change Management Konzept
Result	Pass
Finding	N/A
Relevance	N/A

Table 74 – Examination results: OEV paragraph 23.4

Key	23.5
Requirement	It must be ensured that none of the elements of the client-sided authentication credentials can be systematically intercepted, changed or redirected during transmission. For authentication, measures and technologies must be used that sufficiently minimise the risk of systematic abuse by third parties.
Observation	The examiners understand that this requirement applies to the authentication process of voters on the voting portal. 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). Likely redirection scenarios include the following: » 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. The Post prints the certificate's fingerprint of the voting portal on the voting material and instructs voters to check it to ensure that they have not been redirected to a malicious website. 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. Other countermeasures include secure development practices, use of a Web Application Firewall, performance of regular technical tests (ethical hacking, public code review, etc.). 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. 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.

	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.
Evidence	» Post's ISO 27001 certificate » Post's ISO 27001 Statement of Applicability » https://www.evoting.ch/fr#rules » Einführung DNSSEC für E-Voting » Whitepaper Infrastructure of the Swiss Post Voting System
Result	Pass
Finding	N/A
Relevance	N/A

Table 75 – Examination results: OEV paragraph 23.5

Development and maintenance of information systems

Key	24.2.1
Requirement	An operating manual is created that includes the following for each user role: » 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	The examiners understand that this requirement applies to the user roles of the e-voting system itself, and therefore exclude the users defined at the infrastructure level from their analysis. During the examination process, the Post referred to the operational guide it has issued at the attention of the cantons as a compliance means with this requirement. The document lists and indicates the purpose of the various hardware and software components needed to organise and

	manage an election event. Hardware includes notebooks, data carriers and smartcards, whereas software includes applications and scripts to be run on the notebooks (either developed by the Post or third-party applications), as well as web portals (voter portal and administration portal). The operational guide also details the step-by-step procedures to be followed by the cantons to manage the whole lifecycle of a ballot. Advice is provided when precautions need to be taken to preserve the security of information during the execution of the procedures. The roles depicted in the operational guide include: » Administration board's members (a.k.a. administrators); » The electoral authority members (a.k.a. commission members); » The system operator (i.e. the Post). The prerogatives of each party are not clearly defined in the document. Only vague indications were found by the examiners such as: "[…] setting up the election event only requires the presence of the administrators, whereas releasing the election event also requires the presence of the electoral authority", or "To constitute the Electoral authority, The Administration board must be active in the Secure Data Manager". An additional role exists without being mentioned explicitly, assumed by the intended readers of the operational guide, i.e., the personnel in charge of configuring and operating the e-voting system when an election event occurs. The *e-voting.ch* portal, as well as the cantons' e-voting landing pages and help pages provide security advice to the voters and instructions in case of difficulties encountered or malfunction. The voting material contains detailed instructions regarding the verification steps to be performed during the voting process to ensure no fraud nor issue takes place.
Evidence	» E-voting operational guide » evoting.ch » Sample voting material » Cantons' e-voting landing page / Voting portal help page
Result	Fail
Finding	At the exception of succinct recommendations proposed throughout the operational guide, that may be considered as "a description of the security measures to be implemented in order to achieve the operational security objectives", the operational guide does not include the elements forming the requirement 24.2.1.
Relevance	N/A

Table 76 – 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	The operating manual document itself does not include this information. It only contains a procedure that is followed in the event of an error, which mentions that the e-voting system is put in maintenance mode while the incident is dealt with. A separate document (*Emergency Notfallhandbuch*) describes the organisation adopted by the Post in case of an emergency event affecting the e-voting system. A decision matrix (*Ereignisentscheidungsmatrix*) details the steps to take according to the nature of the emergency. The e-voting team maintains a knowledge base of common errors likely to affect the e-voting system's components, including the step by step associated procedures to troubleshoot and fix the issues.
Evidence	» E-voting operational guide » Emergency Notfallhandbuch » Ereignisentscheidungsmatrix » Wikit.post.ch
Result	Fail
Finding	The operational guide itself does not include the elements necessary to satisfy the requirement 24.2.2
Relevance	N/A

Table 77 – Examination results: OEV paragraph 24.2.2

Key	24.2.3
Requirement	The operating manual must be precise and fit for purpose.
Observation	The Post offers the possibility for the cantons to submit requests for improvements via a ticketing system. In addition, its operational guide has been designed by user experience specialists in order to maximise its readability. However, given that it does not include all the ordinance's requirements, the examiners cannot state that it is "precise" nor "fit for the purpose".
Evidence	E-voting operational guide
Result	Fail
Finding	Given that the Post's operational guide does not include all the OEV's requirements specified in requirements 24.2.1 and 24.2.2, it can hardly be qualified as "precise" nor "fit for the purpose", although it is subject to continuous improvement and readability efforts.

Relevance	N/A

Table 78 – Examination results: OEV paragraph 24.2.3

Key	24.3.1
Requirement	The preparation process describes all the steps necessary for: » 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 examiners understand the term “preparation process” as the preparation of the e-voting systems for an election event. The Post maintains a detailed description of the e-voting components’ preparation process on its internal wiki, marked by quality gates. Acceptance of the delivery procedure is performed using checklists to validate every quality gate and ensure that setting up the e-voting environment is performed in respect of information security good practices. The installation of the software itself follows a formal release management process that includes security testing prior to acceptance.
Evidence	» E-voting operational guide » FR 20210730 Checklist Quality Gates 0.8 Simulation » Release management Service E-Voting » E-Voting Urnengang Vorbereitung Prozess
Result	Pass
Finding	N/A
Relevance	N/A

Table 79 – 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 release management process adopted for the e-voting software delivery requires the following to be documented: » Change requests, under the form of a product backlog; » Analysis of security findings gathered from various sources (e.g. security tests, security bug reports, etc.); » Security findings requiring a treatment; » Releases documentation;

	» Acceptance test reports; » Release notes. The Post maintains a “release overview cockpit” informing the internal stakeholders of the status of on-going releases. Releases are submitted to security testing as described in the *Test Concept of the Swiss Post Voting System* document available on the e-voting Gitlab instance. The examiners estimate that the release practices employed by the Post are aligned with good information security practices.
Evidence	» Release management Service E-Voting » https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/Testing/Test Concept of the Swiss Post Voting System.md
Result	Pass
Finding	N/A
Relevance	N/A

Table 80 – Examination results: OEV paragraph 24.3.2

Key	24.3.3
Requirement	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: » 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	The Post has developed a “trusted build concept” to meet those requirements. It is based on a reproducible model: To provide evidence that the executable code has been compiled from the sources made available to the public for review, the Post provides detailed indications on its public source code repository for the community to be able to rebuild the source code in the same exact conditions. The artefacts’ hashes values can then be compared. However, the frontend artefacts are currently not part of the trusted build, as the build pipeline is not entirely deterministic. Third party libraries used by the e-voting system are scanned against vulnerabilities during the build process and the scan results are reviewed for action. The build process is performed under the supervision of an independent observer to ensure that the artefacts’ hashes are genuine. At the time of the examination, the trusted build concept has not been entirely formalised, nor subject to an end-to-end execution. As a result, the examiners are not able to state that the requirement is met.
Evidence	https://gitlab.com/swisspost-evoting/e-voting/e-voting/-/blob/master/README.md#Reproducible-Builds
Result	Fail
Finding	At the time of the examination, the trusted build concept developed by the Post to carry out a reliable and verifiable compilation of the e-voting applications’ source code with appropriate security measures has not been entirely formalised, nor been subject to an end-to-end execution. The examiners are therefore not able to state that the executable code of the e-voting system is a verifiable and faithful representation of the source code which has been subjected to public scrutiny and independent examinations, and that its compilation allows a chain of proofs.
Relevance	N/A

Table 81 – Examination results: OEV paragraph 24.3.3

Key	24.3.4
Requirement	A reliable and verifiable deployment with appropriate security measures must be carried out. This is to ensure that: 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. The deployment allows a chain of proofs to be created for the verification of the software and includes in particular: » 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	There is no process in place to provide evidence that the software deployed into the production environment is the one that has been subject to public scrutiny, nor that the production environment conforms to that which has been subjected to public scrutiny and independent examinations. The business parameters introduced are listed in the *Operational Guide* document. They include: » The time period for the election event; » The electoral authority; » The number of counting circles for Swiss abroad (optional); » The voting and election order (optional). The parameters are reviewed for accuracy on day 1 of the election by the cantons. As those parameters are inputted in an xml file (param.xml), the examiners estimate that the review of the values by the cantons provides assurance that the said values do not render the system vulnerable. When preparing an election event, technical parameters need to be inputted: The generation of the encryption parameters requires a seed (a 256-bit long number). The operational guide mentions that a seed needs to be defined. The seed is generated by the cantons. The operational guide does not mention a step in the procedure to verify that the seed has the minimal required length. A file containing prime numbers (to be associated to the voting options) is also uploaded, as well as the signature of this file. The origin of those elements is not known by the examiners. The examiners cannot conclude that evidence exists, that the technical parameters introduced do not render the system vulnerable.
Evidence	E-Voting operational guide
Result	Fail
Finding	There is no process in place to provide evidence that the software deployed into the production environment is the one that has been subject to public scrutiny, nor that the production environment conforms to that which has been subjected to public scrutiny and independent examinations. The examiners did not find any evidence that the technical parameters (relating to the cryptographic protocol) imputed by the cantons during the preparation of an event do not render the system vulnerable.
Relevance	N/A

Table 82 – 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	The trusted build concept elaborated by the Post includes the presence of two observers to witness the reliable and verifiable compilation of the e-voting system's source code: a representative of the canton and an independent contractor. However, the examiners were not provided with evidence that a similar organisation is planned at this stage to witness the deployment of the compiled software. Nor were they provided with technical procedures guaranteeing a reliable and verifiable deployment of the e-voting software.
Evidence	https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/Operations/Trusted Build of the Swiss Post Voting System.md
Result	Fail
Finding	There is currently no documented process to support an independent observation of the deployment process into the production environment.
Relevance	N/A

Table 83 – Examination results: OEV paragraph 24.3.5

Key	24.3.6
Requirement	The chain of evidence of reliable and verifiable compilation and deployment is made publicly available.
Observation	The trusted build concept process includes the publication of the compiled software artefacts hash values, enabling a reliable and verifiable compilation. No chain of evidence exists at this stage to ensure the reliable and verifiable nature of the software deployment phase. As the trusted build concept has not been subject to end-to-end execution at this stage, the artefacts hash values are not published yet.
Evidence	N/A
Result	Fail
Finding	No chain of evidence exists at this stage to ensure the reliable and verifiable nature of the software deployment phase.

	As the trusted build concept has not been subject to end-to-end execution at this stage, the chain of evidence of reliable and verifiable compilation is not published yet.
Relevance	N/A

Table 84 – Examination results: OEV paragraph 24.3.6

Key	24.4.1
Requirement	Processes are defined for the correction of flaws. The processes include: » documentation of specific aspects, in particular with regard to the traceability of flaws for all versions of the software, and of the methods used to ensure that system users have information on flaws, corrections and possible corrective actions; » the obligation to describe the nature and impact of all security flaws, information on the status of work to find a solution and the corrective measures adopted; » a description of how system users can make reports and enquiries about suspected flaws in the software known to the software developers; » a procedure requiring a timely response and automatic dispatch of security flaw reports and appropriate corrective actions to registered system users who may be affected by the flaw.
Observation	The Post provides public access to the e-voting system's source code, allowing the community to look for vulnerabilities affecting it. The Post has opened a bug bounty program. Submissions can be performed directly to the Post's e-voting team or via a third-party bug bounty platform. The process for the correction of flaws is formalised and follows three steps: » Triage of reports. At this stage, submissions are tracked and dispatched for analysis; » Validation of findings: The submission is validated, its description is improved if needed, and its criticality is estimated; » Communication. The vulnerability resolution strategy is defined and communicated. A dedicated website provides information to the interested program participants. Validated vulnerabilities are published on a publicly available Gitlab instance, detailing the nature of the flaw, its possible impact, its current status. When identified flaws concern the code, the development team publishes software increments on a dedicated branch (*develop*) of its public Gitlab instance, to make the changes in the source code easier to understand. Flaws affecting the e-voting system are also reported through the Post's internal security assessment process, which is applied at regular intervals. Identified vulnerabilities are also subject to publication on the e-voting dedicated Gitlab instance.
Evidence	» Process E-Voting QCV Quellen triangieren

	» Process E-Voting QCV Tickets, Findings validieren » Process E-Voting QCV PO – Kommunikation und Publizierung sicherstellen » https://gitlab.com/groups/swisspost-evoting/-/issues » https://evoting-community.post.ch/ » https://yeswehack.com/programs/swiss-post-evoting » Software development process of the Swiss Post Voting System » https://gitlab.com/swisspost-evoting/e-voting/e-voting/-/commits/develop » Handbuch ICT-Security Assessments » Sicherheitslücken proaktiv bearbeiten (Security Change / Patch Management)
Result	Pass
Finding	N/A
Relevance	N/A

Table 85 – Examination results: OEV paragraph 24.4.1

Key	24.4.2
Requirement	A process is defined for handling reported flaws. This process ensures that all reported and confirmed flaws are corrected and that the procedures for correction are communicated to system users. It provides for arrangements to ensure that the correction of security flaws does not give rise to new security flaws.
Observation	The process for handling the reported flaws is formalised and follows three steps: triage of reports, validation of findings and communication. The status of reported flaws is published on a dedicated public Gitlab instance and updated once the corrections are implemented. The correction of flaws follows the formal e-voting change management and release management processes, which address the risk of introducing new security flaws.
Evidence	» https://gitlab.com/groups/swisspost-evoting/-/issues » E-Voting Change Management Konzept » Release management Service E-Voting » Process E-Voting QCV Quellen triangieren » Process E-Voting QCV Tickets, Findings validieren » Process E-Voting QCV PO – Kommunikation und Publizierung sicherstellen
Result	Pass
Finding	N/A
Relevance	N/A

Table 86 – Examination results: OEV paragraph 24.4.2

Key	24.4.3
Requirement	Policies must be defined for the reporting and correction of flaws. These include: » 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	The e-voting Gitlab instance, as well as a dedicated web site maintained by the Post, provide detailed instructions at the attention of persons interested to look for vulnerabilities and submit them, or to communicate with the e-voting development team.
Evidence	» https://gitlab.com/groups/swisspost-evoting/-/issues » https://evoting-community.post.ch/
Result	Pass
Finding	N/A
Relevance	N/A

Table 87 – 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	The Post provides training to its own employees who work within the teams involved in the operation of the e-voting infrastructure, as well as to the cantons. E-voting employees' training is part of the onboarding process and is performed at the team level. Comprehensive documentation is available on the e-voting dedicated internal wiki. When onboarding a canton, the Post also trains the administrators of the e-voting system on the cantons side in a "train the trainer" mode (i.e. so that trained people are in turn able to train their own colleagues). The *Operational Guide* is the main document aimed at the persons who operate and use the system.
Evidence	» Eintritt-Checklist_I351 » Eintritt-Checklist_I353

	» Eintritt-Checklist_I354 » Eintritt-Checklist_I356 » wikit.post.ch » Schulungskonzept E-Voting » Training concept canton » E-voting operational guide
Result	Partial fail
Finding	The document *Schulungskonzept E-Voting* is not up to date (the version provided to the examiners is dated May 2019 and mentions the company Scytl for 3rd level support, whereas this company no longer exists).
Relevance	N/A

Table 88 – Examination results: OEV paragraph 25.6.2

Key	25.6.3
Requirement	Training includes the opportunity to train on a system designed for training purposes.
Observation	The 2-day training provided by the Post when onboarding a canton is supported by a test environment (either the canton's test environment if existing, or a test environment provided by the Post). The notebooks necessary to manage an election event are provided by the Post.
Evidence	» Training concept canton » Schulungskonzept E-Voting
Result	Pass
Finding	N/A
Relevance	N/A

Table 89 – Examination results: OEV paragraph 25.6.3

Key	25.6.4
Requirement	Help on using the system must be readily available.
Observation	The *Operational Guide* is the main document providing help on using the system. The Post is also developing a dedicated collaboration platform on e-voting with the cantons, including frequently asked questions (FAQ's) and help checklists. 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).

	The cantons have the possibilities to submit feedback regarding the documentation in an issue tracking system for continuous improvement purpose.
Evidence	» E-voting operational guide » Schulungskonzept E-Voting
Result	Partially fail
Finding	The document *Schulungskonzept E-Voting* is not up to date: It provides links to Scytl documentation (whereas the company no longer exists), located on a decommissioned document sharing platform. At the time of the examination, the collaboration platform between the Post and the cantons for e-voting-related topics is under development.
Relevance	N/A

Table 90 – Examination results: OEV paragraph 25.6.4

5 Summary of findings and recommendations

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

Key	2.5
Finding	The soundness of the proof in accordance with Article 5 paragraph 2 is based on the trustworthiness of a component considered untrustworthy (i.e., the voting server), the trustworthiness of the procedure for distributing the voting papers and the trustworthiness of the procedure for requesting information for the cantons. Therefore, the examiners cannot confirm the exclusive nature of the requirements set in Article 6 letters a and b.
Recommendation	The examiners estimate that compliance with this requirement is practically not achievable. They suggest that the Chancellery consider their observation and, if deemed relevant, update the requirement accordingly. Furthermore, the identified discrepancy between the OEV and the *Protocol of the Swiss Post Voting System v0.9.11* document regarding the trustworthy nature of the voting server should be analysed.

Table 91 – Findings and recommendations related to requirement 2.5

Key	3.6
Result	Partially fail
Finding	The installation procedure of the e-voting software on the control component is currently not formalised. Therefore, the examiners cannot ascertain that it is performed in an observable manner.
Recommendation	Formalise the installation procedure in an observable manner of the e-voting software on control components.

Table 92 – Findings and recommendations related to requirement 3.6

Key	3.14
Result	Partially fail
Finding	The monitoring systems for the control components are not distinct from each other. The Post’s datacentre service team has the keys for all control components’ racks.
Recommendation	Strict adherence to this requirement would require deploying distinct instances of the monitoring systems. In the examiners’ opinion, however, the cost induced by such an evolution (in terms of

	infrastructure, software and personnel) seems disproportionate in regard to its risk reduction potential. The Post should assess whether a stricter segregation of physical access rights to the control components' racks is feasible from an operational point of view and is relevant from a security perspective (i.e. the measure has a low investment/risk reduction ratio).

Table 93 – Findings and recommendations related to requirement 3.14

Key	3.16
Result	Partially fail
Finding	The current Oracle database hardening reference guide is a rather old document (2014) that covers an older version (i.e., v.11gR2) of the product than the one supporting the e-voting system, in particular its control components. It may therefore not be adapted to the present context.
Recommendation	The Post should update its Oracle database hardening guide to ensure that it is appropriate to the version that runs on the control components.

Table 94 – Findings and recommendations related to requirement 3.16

Key	13.1
Result	Partially fail
Finding	The ISDP concept related to the e-voting system, which serves as a basis for the evaluation of the risks pertaining to the system, is not finalised at this stage. The examiners note that the Post only considers the threats listed in Numbers 13.3-13.39 in the existing document whereas they should be considered as a minimum basis. For instance, threat scenarios involving vandalism or sabotage on physical components of the e-voting system are not considered, nor accidental availability issues / information disclosure resulting from a bad manipulation by an employee.
Recommendation	The Post should formalise the ISDP concept related to the e-voting system. Threat modelling techniques should be used to document thoroughly all possible threats pertaining to the system and derive adequate countermeasures. Consider also the recommendations provided for the findings related to the requirements 15.2, 15.3, 22.1 and 23.2.

Table 95 – Findings and recommendations related to requirement 13.1

Key	14.1
Result	Partially fail

Finding	No alarm is currently set in case of errors in the registration of votes.
Recommendation	Consider defining an alarm in the case of errors in the registration of votes, in order to ease the detection of this type of events.

Table 96 – Findings and recommendations related to requirement 14.1

Key	15.1
Result	Partially fail
Finding	The e-voting system does not implement the requirements of the Post's security policy on cryptography with regards to certificate pinning.
Recommendation	Certificate pinning being no longer considered as a best practice for web applications, the Post should consider revising its policy to fix this compliance issue.

Table 97 – Findings and recommendations related to requirement 15.1

Keys	15.2 & 15.3
Result	Partially fail
Finding	The Post has not formally documented how cryptographic controls implemented within the e-voting system mitigate specific threats at the infrastructure level (e.g. in its ISDS concept or in a threat model).
Recommendation	The Post's ISDS concept or a threat model for the e-voting system should document the usages of cryptography and what threats those usages mitigate.

Table 98 – Findings and recommendations related to requirements 15.2 & 15.3

Key	18.3
Result	Fail
Finding	No evidence was shown to the examiners that the Post's standard supplier security management process has been applied to the companies involved in the e-voting's infrastructure supply chain. Moreover, the document shown to the examiners fails to mention some suppliers (e.g. Postfinance, as the datacentres' provider, which contract is managed directly by PostIT).
Recommendation	The Post should keep an inventory of the suppliers involved in the e-voting supply chain and ensure that each supplier undergoes its supplier security management process.

Table 99 – Findings and recommendations related to requirement 18.3

Key	19.3

Result	Partially fail
Finding	The confidentiality grade mentioned in the *Schutzbedarfanalyse* document for the data processed within the e-voting system does not correspond to the taxonomy used in the information classification policy.
Recommendation	The Post should align the taxonomy for confidentiality between its various documents.

Table 100 – Findings and recommendations related to requirement 19.3

Key	20.1
Result	Fail
Finding	The screening process on human resources interacting with the e-voting system is only performed once, whereas it should be performed every four years, as specified in the Post's guideline.
Recommendation	The Post should ensure that the screening process on human resources interacting with the e-voting system is executed in accordance with its policy (i.e., every four years).

Table 101 – Findings and recommendations related to requirement 20.1

Key	20.2
Result	Fail
Finding	The examiners did not find any evidence that the Post’s human resources department, or any other function assumes the responsibility for guaranteeing the trustworthiness of human resources.
Recommendation	The Post should document in a clear way that the human resources department assumes the responsibility for guaranteeing the trustworthiness of human resources.

Table 102 – Findings and recommendations related to requirement 20.2

Key	21.4
Result	Fail
Finding	The source code of the e-voting system being one of its critical information assets, one cannot state that all data is processed exclusively in Switzerland.
Recommendation	The Post should use a source code repository based in Switzerland to comply with the OEV’s requirements.

Table 103 – Findings and recommendations related to requirement 21.4

Key	22.1
Result	Fail
Finding	Although good practices in terms of allocation of obligations and areas of responsibility exist, a comprehensive documentation detailing how those practices mitigate the various types of risks originating from human resources does not seem to be available at this stage.
Recommendation	The Post should document in detail (for instance, in its ISDP concept for the e-voting system) how apportioning obligations and areas of responsibility for the operation of the e-voting systems mitigates the various types of risks originating from human resources.

Table 104 – Findings and recommendations related to requirement 22.1

Key	23.2
Result	Fail
Finding	At the time of the examination, the ISDP concept does not document the detailed risks and countermeasures related to accesses to the e-voting system's infrastructure and software. The examiners cannot conclude that access to infrastructure and software is regulated and documented in detail on the basis of a risk assessment. Moreover, it seems that it is possible to modify the default settings regarding the minimum number of members within the Administration Board. The examiners are therefore not able to ascertain those manual operations in high-risk areas are conducted by at least two persons.
Recommendation	The Post should document in detail the risks and countermeasures related to accesses to the e-voting system's infrastructure and software, for instance in its ISDP concept. The parameterisation options of the e-voting software should be mapped with the OEV's requirements, e.g., with regards to the minimum number of members within the Administration Board.

Table 105 – Findings and recommendations related to requirement 23.2

Key	24.2.1
Result	Fail
Finding	At the exception of succinct recommendations proposed throughout the operational guide, that may be considered as "a description of the security measures to be implemented in order to achieve the operational security objectives", the operational guide does not include the elements forming the requirement 24.2.1.
Recommendation	The Post should provide the missing information and structure its operational guide in a way that satisfies the requirement 24.2.1.

Table 106 – Findings and recommendations related to requirement 24.2.1

Key	24.2.2
Result	Fail
Finding	The operational guide itself does not include the elements necessary to satisfy the requirement 24.2.2
Recommendation	The Post should provide the missing information and structure its operational guide in a way that satisfies the requirement 24.2.2.

Table 107 – Findings and recommendations related to requirement 24.2.2

Key	24.2.3
Result	Fail
Finding	Given that the Post's operational guide does not include all the ordinance's requirements specified in requirements 24.2.1 and 24.2.2, it can hardly be qualified as "precise" nor "fit for the purpose", although it is subject to continuous improvement and readability efforts.
Recommendation	The Post should provide the missing information and structure its operational guide in a way that satisfies the requirements 24.2.1 and 24.2.2.

Table 108 – Findings and recommendations related to requirement 24.2.3

Key	24.3.3
Result	Fail
Finding	At the time of the examination, the trusted build concept developed by the Post to carry out a reliable and verifiable compilation of the e-voting applications' source code with appropriate security measures has not been entirely formalised, nor been subject to an end-to-end execution. The examiners are therefore not able to state that the executable code of the e-voting system is a verifiable and faithful representation of the source code which has been subjected to public scrutiny and independent examinations, and that its compilation allows a chain of proofs.
Recommendation	The Post should finalise its trusted build concept, considering all the elements mentioned in the requirement 24.3.3.

Table 109 – Findings and recommendations related to requirement 24.3.3

Key	24.3.4
Result	Fail

Finding	There is no process in place to provide evidence that the software deployed into the production environment is the one that has been subject to public scrutiny, nor that the production environment conforms to that which has been subjected to public scrutiny and independent examinations. The examiners did not find any evidence that the technical parameters (relating to the cryptographic protocol) imputed by the cantons during the preparation of an event do not render the system vulnerable.
Recommendation	The Post should develop a process to meet the requirement 24.3.4.

Table 110 – Findings and recommendations related to requirement 24.3.4

Key	24.3.5
Result	Fail
Finding	There is currently no documented process to support an independent observation of the deployment process into the production environment, nor any technical procedures guaranteeing a reliable and verifiable deployment.
Recommendation	The Post should formalise a process or technical procedures to meet the requirement 23.4.5.

Table 111 – Findings and recommendations related to requirement 24.3.5

Key	24.3.6
Result	Fail
Finding	No chain of evidence exists at this stage to ensure the reliable and verifiable nature of the software deployment phase. As the trusted build concept has not been subject to end-to-end execution at this stage, the chain of evidence of reliable and verifiable compilation is not published yet.
Recommendation	The Post should perform an end-to-end execution of its trusted build concept and publish the chain of evidence of reliable and verifiable compilation. The process to be developed for a reliable and verifiable deployment of the e-voting software should include the publication of relevant evidence.

Table 112 – Findings and recommendations related to requirement 24.3.6

Key	25.6.2 & 25.6.4
Result	Partially fail

Finding	The document *Schulungskonzept E-Voting* is not up to date (the version provided to the examiners is dated May 2019 and mentions the company Scytl for 3rd level support, whereas this company no longer exists).
Recommendation	The Post should update the document in order to reflect the current status with regards to e-voting training.

Table 113 – Findings and recommendations related to requirement 25.6.2 & 25.6.4

Key	25.6.4
Result	Partially fail
Finding	The document *Schulungskonzept E-Voting* is not up to date (the version provided to the examiners is dated May 2019 and mentions the company Scytl for 3rd level support, whereas this company no longer exists).
Recommendation	The Post should finalise the development of its collaboration platform with the cantons related to e-voting and release it.

Table 114 – Findings and recommendations related to requirement 25.6.4

6 References

[1] "Reorienting eVoting and ensuring stable trial operation," *www.egovernment.ch*. https://www.egovernment.ch/en/umsetzung/schwerpunktplan/vote-electronique/ (accessed Oct. 21, 2021).

[2] Swiss Federal Chancellery, Political Rights Section, "Redesign and relaunch of trials - Final report of the Steering Committee Vote électronique (SC VE)." Nov. 30, 2020. Accessed: Dec. 06, 2021. [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

[3] Swiss Federal Chancellery, Political Rights Section, "Partial revision of the Ordinance on Political Rights and total revision of the Federal Chancellery Ordinance on Electronic Voting (Redesign of Trials)." Apr. 28, 2021. Accessed: Dec. 06, 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

[4] Swiss Federal Chancellery, "Federal legislation." https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/versuchsbedingungen.html (accessed Oct. 21, 2021).

[5] Swiss Federal Chancellery (FCh) - Political Rights section, "Audit concept for examining Swiss Internet voting systems - v1.3." May 18, 2021.

[6] Swiss Federal Chancellery, "Federal Chancellery ordinance on electronic voting (OEV)." Apr. 28, 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

[7] Swiss Post, "UP2021 - Mapping List VEleS.xlsx." Jul. 13, 2021.

7 Appendices

7.1 Appendix: interview sessions log

Date	Topic	Participants Swiss Post
14.09.2021	End-to-End election process	Matthieu Troehler
17.09.2021	End-to-End election process	Matthieu Troehler
21.09.2021	Initialisation	Matthieu Troehler, Philipp Hunziker
24.09.2021	Physical security	Matthieu Troehler, Sascha Wyss
08.10.2021	Service operation	Matthieu Troehler, Daniel Stucki
15.10.2021	Infrastructure	Matthieu Troehler, Philipp Hunziker, Daniel Stucki
02.11.2021	HR & maintenance	Matthieu Troehler, Philipp Hunziker, Lukas Ruggli
05.11.2021	Voters information	Matthieu Troehler
09.11.2021	Risk management	Martin Sax, Martin Stingelin, Matthieu Troehler, Philipp Hunziker
14.11.2021	Compliance	Matthieu Troehler, Philipp Hunziker
19.11.2021	Trusted build	Matthieu Troehler, Philipp Hunziker, Thomas Caldara, Patrick Oliveira Andrade
19.11.2021	ISDP concept	Anastasija Beeler, Martin Sax, Xavier Monnat, Matthieu Troehler, Philipp Hunziker
23.11.2021	Incident Management	Matthieu Troehler, Philipp Hunziker, Pilippe Oesch
31.12.2021	Follow-up on open points	Matthieu Troehler
24.01.2022	Follow-up on open points	Matthieu Troehler, Philipp Hunziker
02.02.2022	Follow-up on open points	Matthieu Troehler
03.02.2022	Follow-up on ISDP concept / risk management	Anastasija Beeler, Martin Sax, Martin Stingelin, Delal Kaygisiz.

Table 115 - Interview sessions log