Cyberdefense

Federal Chancellery

Examination of the Swiss Internet voting system

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

23 May 2025

Contact information

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

Contributors

Name	Role
Stéphane Adamiste	Chief Product Officer, Orange Cyberdefense Switzerland

Document history

Version	Date	Author	Change details
0.1	17 March 2025	Stéphane Adamiste	Working version
1.0	16 April 2025	Stéphane Adamiste	Released version
1.1	23 may 2025	Stéphane Adamiste	Integration of feedback from the cantons

Contents

Management summary

Context, scope and objective of the examination

The objective of this examination was to assess to which extent the infrastructure operated, and the organisational measures implemented by the Abraxas print office (in charge of printing and packaging the polling cards, on behalf of the cantons of Basel-Stadt, Graubünden, St Gallen and Thurgau, in the context of electronic voting) satisfy a subset of requirements (audit scope 3 - Infrastructure and operation, c) Assess the infrastructure and organisational measures of the print office) set forth by the Federal Chancellery's ordinance on e-voting. In total, the examination included 45 criteria.

Methodology

The examiners looked for evidence of effort to comply with said criteria by conducting interviews with Abraxas personnel responsible for setting up and operating the infrastructure used to print and package the polling cards, by analysing the related documentation (i.e., policies, procedures, specifications, reports, processes, etc.) and by performing a physical inspection of the print office's facilities (on February 20th, 2025)

Results

During this examination, the Abraxas print office was able to demonstrate a high level of compliance with the requirements of the Ordinance on Electronic Voting. While one audit criterion was not fully met — namely, that the packaging of printed polling cards is not systematically performed immediately after printing — the compensatory measure implemented by the print office to mitigate the associated risks was deemed satisfactory by the auditors.

Final note

The examiners conclude this summary by thanking the Abraxas print office, the cantons of Basel-Stadt, Graubünden, St. Gallen and Thurgau 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.

1 Context

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

7. Orange Cyberdefense Switzerland (“OCD CH”, formerly SCRT) was mandated by the Federal Chancellery to assess the compliance of the print offices involved in the printing and packaging of the e-voting material on behalf of the cantons, against the applicable requirements of the OEV (*Scope 3: Infrastructure and operation, c) Assess the infrastructure and organisational measures of the print office*). [8] [9]
8. In September 2022, an updated version of the audit concept was issued by the Federal Chancellery [10].
9. In 2025, OCD CH was once again mandated by the Federal Chancellery to perform a new, full-scope audit of the e-voting system provided by the Post. On this occasion, the Federal Chancellery updated its audit concept to include additional requirements [11].

2 Methodology

2.1 Process

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

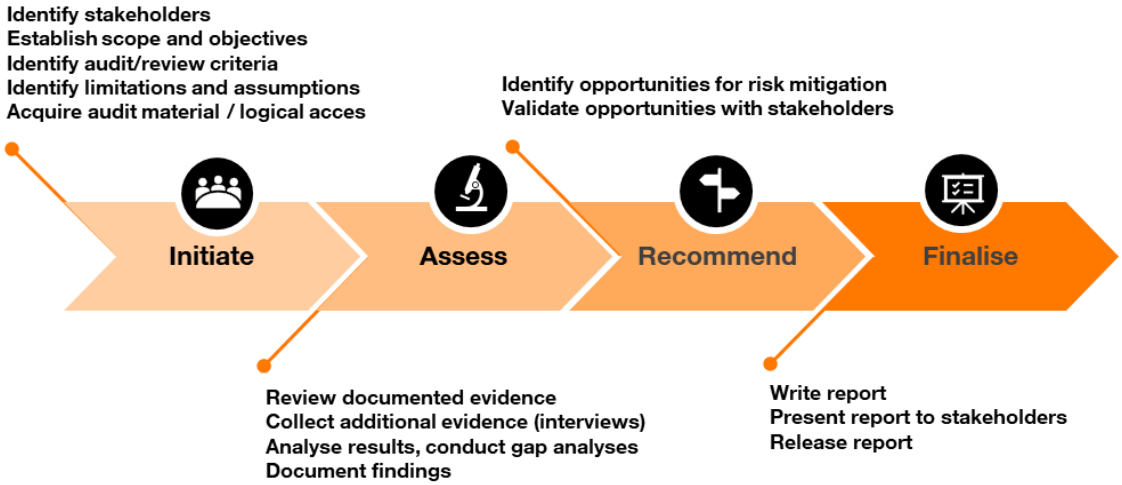

Figure 1: Examination process

2.2 Collection of evidence

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

2.3 Findings

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 findings indicated in this report only reflects the opinion of the examiners and may be subject to re-evaluation from relevant parties.

2.5 Relevance of the assessment criteria

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. The observation of the actual implementation of the OEV's requirements within the e-voting system was limited to the demo made by the e-voting representatives of the Thurgau canton carried out to verify the accuracy of the examinees' statements.

2.6.2 Enforcement of security measures

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 from the print offices' standpoint against the following criteria:

Cryptographic protocol requirements for complete verifiability

Key	Requirement
2.9.1.2	**For soundness of the proofs referred to in Number 2.5** The following system participants may be considered trustworthy: ■ set-up component ■ print component ■ one of four control components per group, leaving open which one it is
2.9.3.2	**For preserving voting secrecy and excluding premature partial results in accordance with Number 2.7** The following system participants may be considered trustworthy: ■ set-up component ■ print component ■ user device ■ one of four control components per group, leaving open which one it is
2.9.4.2	**For preserving voting secrecy and excluding premature partial results in accordance with Number 2.8** The following system participants may be considered trustworthy: ■ set-up component ■ print component ■ user device ■ one of four control components per group, leaving open which one it is
2.13.3	**Requirements for the definition and description of the cryptographic protocol** It may be assumed that trustworthy channels exist to distribute electronic certificates among system participants. Number 3.8 applies.

Table 1 - E-voting requirements: Cryptographic protocol requirements for complete verifiability

Trustworthy components in accordance with Number 2 and for their operation

Key	Requirement
3.5	With the exception of the components mentioned under Numbers 3.1 and 3.3, the canton may delegate the operation of any part of the system, including the control components and the print component, to private service providers. A private operator of the print component may only perform operational tasks that are required for preparation, packaging and delivery.
3.6	Trustworthy components (set-up components, print components, auditors' technical aids and control components) must be set up, updated, configured and secured in an observable process.
3.7	Before installing software, all programs must be checked using an official and trustworthy reference to ensure that the files are the correct and unaltered version.

Key	Requirement
3.8	When other system participants' electronic certificates are installed, their authenticity must be ensured. To that end, there should be a manual process in which people transfer the electronic certificates from one machine to another via a physical data carrier in accordance with 3.13.
3.9	The timing for updating all software of trustworthy components must be such that the expected benefits outweigh the potential hazards.
3.10	Set-up components, print components and auditors' technical aids that are involved in any way in the processing of critical data must be physically monitored during the entire computing time by two persons and until any critical data have been deleted or securely stored. At most, they may be interconnected by visible physical cables so that it is as evident as possible that no other machines can access them until the confidential data is destroyed.
3.11	Trustworthy components may not be connected to the Internet when installing or updating software.
3.12	In principle, critical data must be destroyed after use. If there are good reasons, secure storage of the data carrier is also permitted as an alternative.
3.13	Data exchange or storage media, such as USB flash drives, must be removed after the data has been uploaded to the trustworthy components and may only be reused before the data is destroyed if there was no critical data on the trustworthy component before the data was uploaded. Data exchange or storage media must be reformatted and any data on them must be destroyed before they are used with the aid of a component operated in accordance with the requirements for trustworthy components.
3.14	Logical or physical access to trustworthy components or data carriers containing critical data must be impossible without another person becoming aware of it, for example by having to assist in granting access (strict two person principle).
3.17	Trustworthy components may perform only the intended operations.
3.19	All procedures for dealing with trustworthy components must be documented in writing and in a manner that is easily understood by the persons concerned.
3.20	Any access to and use of a trusted component or data carrier containing critical data must be logged.

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

Requirements for printing offices

Key	Requirement
7.1	The printing data used to produce the polling cards are transmitted encrypted and signed. Alternatively, a data carrier containing this data may be delivered in person. In this case, the data carrier must be transported and delivered to the printing office by two persons, who must both stay with the data carrier until it is delivered.
7.2	The encryption must meet the requirements of eCH standard 0014, Chapter 7.5. If encryption is symmetric, the secret decryption key is sent to the persons responsible at the printing office via a secure secondary channel.
7.3	The person responsible at the printing office who receives the data carrier must sign an acknowledgement of receipt.

Key	Requirement
7.4	For the data carrier containing the print data, the component on which the critical data is decrypted and all components that process the critical data, the provisions for the print component as set out in Number 3 apply.
7.5	The persons responsible at the print office carry out a material quantity check.
7.6	After printing the polling cards, the print office must destroy the data received.
7.7	If the print office also carries out the packaging and dispatch of the polling cards, these must be packaged together with the voting papers immediately after printing.
7.8	The channel between the printing office and the voters may only be considered trustworthy if the bodies responsible under cantonal law deliver the packaged voting papers to the voters by post or ensure that it is handed over in person.

Table 2 - E-voting requirements: Requirements for printing offices

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

Key	Requirement
14.9	All parts of the voting system must be regularly updated in a predetermined and documented process in order to eliminate weaknesses that have become known.

Table 3 - E-voting requirements: Identifying and reporting security events and vulnerabilities; dealing with security events and making security improvements

Organisation of information security

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

Table 4 - E-voting requirements: Organisation of information security

Management of intangible and tangible resources

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

Key	Requirement
	resource is assigned a person who takes responsibility for it.
19.2	The acceptable use of intangible and tangible resources must be defined.
19.3	Classification guidelines for information must be issued and communicated.
19.4	Procedures must be devised for the labelling and handling of information.

Table 5 - E-voting requirements: Management of intangible and tangible resources

Trustworthiness of human resources

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

Table 6 - E-voting requirements: Trustworthiness of human resources

Physical and environment security

Key	Requirement
21.1	The security perimeters of the various premises of the infrastructure are clearly defined.
21.2	For physical entry to these various infrastructure premises, entry controls must be defined, implemented and appropriately checked.
21.3	To guarantee the security of devices within and outside the infrastructure premises, appropriate policies and procedures must be defined and compliance therewith monitored and reviewed.
21.4	All data must be processed and in particular stored exclusively in Switzerland.

Table 7 - E-voting requirements: Physical and environment security

Management of communication and operations

Key	Requirement
22.1	Obligations and areas of responsibility must be apportioned so that the risks originating from human resources relating to operations and communications are reduced to residual risks that are compatible with the risk acceptance criteria.
22.2	Appropriate measures must be taken to protect against malware.
22.3	A detailed plan for data backup must be prepared and implemented. The data backup must be regularly reviewed to check that it is functioning correctly.
22.4	Appropriate measures must be defined and implemented to protect the network from the threats listed in the risk assessment in accordance with Article 4 and in connection with Number 13 and for the security of network services.

Key	Requirement
22.5	The procedures for using removable data carriers and for disposing of data carriers must be regulated in detail.

Table 8 - E-voting requirements: Management of communication and operations

4 Examination results

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

Requirement for the cryptographic protocol: individual verifiability

The requirements in sections 2.9 describe which components can be considered trustworthy and which cannot. These requirements are taken into account when auditing the requirements in section 3, which relate to trustworthy components.

Key	2.9.1.2
Requirement	**For soundness of the proofs referred to in Number 2.5** The following system participants may be considered trustworthy: ■ set-up component ■ print component ■ one of four control components per group, leaving open which one it is
Observation	This requirement is taken into account when auditing requirements about trustworthy components. (See Number 3).
Evidence	N/A
Result	N/A
Finding	N/A
Relevance	N/A

Table 9 – Examination results: OEV paragraph 2.9.1.2

Key	2.9.3.2
Requirement	**For soundness of the proofs referred to in Number 2.6** The following system participants may be considered trustworthy: ■ one of four control components per group, leaving open which one it is ■ one auditor in any group, leaving open which auditor it is ■ one technical aid from a trustworthy auditor, leaving open which aid it is
Observation	This requirement is taken into account when auditing requirements about trustworthy components. (See Number 3).
Evidence	N/A
Result	N/A
Finding	N/A
Relevance	N/A

Table 10 – Examination results: OEV paragraph 2.9.3.2

Key	2.9.4.2
Requirement	**For preserving voting secrecy and excluding premature partial results in accordance with Number 2.8** The following system participants may be considered trustworthy: ■ set-up component ■ print component ■ user device ■ one of four control components per group, leaving open which one it is
Observation	This requirement is taken into account when auditing requirements about trustworthy components. (See Number 3).
Evidence	N/A
Result	N/A
Finding	N/A
Relevance	N/A

Table 11 – Examination results: OEV paragraph 2.9.4.2

Key	2.13.3
Requirement	**Requirements for the definition and description of the cryptographic protocol** It may be assumed that trustworthy channels exist to distribute electronic certificates among system participants. Number 3.8 applies.
Observation	This requirement is taken into account when auditing requirements about trustworthy components. (See Number 3).
Evidence	N/A
Result	N/A
Finding	N/A
Relevance	N/A

Table 12 – Examination results: OEV paragraph 2.13.3

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

Key	3.5
Requirement	With the exception of the components mentioned under Numbers 3.1 and 3.3, the canton may delegate the operation of any part of the system, including the control components and the print component, to private service providers. A private operator of the print component may only perform operational tasks that are required for preparation, packaging and delivery.
Observation	The voting material is printed by specialised external third parties. They only perform operational tasks required for preparation, packaging and delivery.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1

Result	■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9
	Pass
	N/A
	N/A

Table 13 – 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 trustworthy components of this print office are the following: ■ A dedicated physical e-voting server ("E-Voting-Server") hosting: ● a virtual machine running the Domtrac software for enriching the polling cards (i.e., inclusion of a datamatrix code for traceability purpose); ● a virtual Prisma server for driving the printer; ■ A Canon Colorstream 3700z printer. According to the documented process, setup up, updates and configurations of trustworthy equipment are performed by two employees of Abraxas or, if necessary, by a technician of the supplier, under the supervision of an Abraxas employee. The equipment is not connected to the Internet. Changes are documented and approved by Abraxas' Change Advisory Board.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.5 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.6 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.6 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.6
Result	Pass
Finding	N/A
Relevance	N/A

Table 14 – Examination results: OEV paragraph 3.6

Key	3.7
Requirement	Before installing software, all programs must be checked using an official and trustworthy reference to ensure that the files are the correct and unaltered version.
Observation	According to the documented process, all software is downloaded from the supplier's official source and the integrity is verified with a hash or other control information. The control information is documented in the change report.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §3.2

	■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §3.3 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §3.3 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §3.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 15 – Examination results: OEV paragraph 3.7

Key	3.8
Requirement	When other system participants' electronic certificates are installed, their authenticity must be ensured. To that end, there should be a manual process in which people transfer the electronic certificates from one machine to another via a physical data carrier in accordance with 3.13.
Observation	According to the documented process, the certificate used to sign the PDF files of the polling cards is delivered through the same channel as the files themselves (i.e., a web portal). The fingerprint of the certificate is either verified in person or transmitted using a secure messaging application (*Threema*) and then verified in an online meeting.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.2 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.3 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.3 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 16 – Examination results: OEV paragraph 3.8

Key	3.9
Requirement	The timing for updating all software of trustworthy components must be such that the expected benefits outweigh the potential hazards.
Observation	According to the documented process, the software of the printing devices is updated following the schedule of the concerned manufacturer. No updates are performed during the period were polling cards are printed.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §3.2 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §3.2 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §3.2

	■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §3.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 17 – Examination results: OEV paragraph 3.9

Key	3.10
Requirement	Set-up components, print components and auditors' technical aids that are involved in any way in the processing of critical data must be physically monitored during the entire computing time by two persons and until any critical data have been deleted or securely stored. At most, they may be interconnected by visible physical cables so that it is as evident as possible that no other machines can access them until the confidential data is destroyed.
Observation	All steps of the printing process are carried out by at least two persons. Critical data is deleted at the end of the printing process. Abraxas maintains a physical server dedicated to e-voting printing operations, which is connected exclusively to the printer through a labelled cable for generating polling cards.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.5 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.6 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.6 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.6
Result	Pass
Finding	N/A
Relevance	N/A

Table 18 – Examination results: OEV paragraph 3.10

Key	3.11
Requirement	Trustworthy components may not be connected to the Internet when installing or updating software.
Observation	According to the documentation, the systems are not connected to Internet when installing or updating software. Patches are installed using USB sticks.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §3.1 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §3.1 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §3.1 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §3.1
Result	Pass

Finding	N/A
Relevance	N/A

Table 19 – Examination results: OEV paragraph 3.11

Key	3.12
Requirement	In principle, critical data must be destroyed after use. If there are good reasons, secure storage of the data carrier is also permitted as an alternative.
Observation	The USB stick containing the encrypted critical data (i.e., the polling cards) is stored encrypted in a safe following the 4-eye principle. The disks containing the images of the Output Management System (Domtrac) and the print server (Prisma) are stored in a secure safe. For each ballot, dedicated virtual machine instances of both systems are created on the physical print server's runtime datastore using these images. The polling cards are then imported from the USB stick, decrypted, and sent to the printer. Secure deletion of the USB stick and the runtime datastore is performed upon written instruction from the cantons, once they have formally accepted the printed materials.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.5 steps 11, 12 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.6 steps 11, 12 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.6 steps 11, 12 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.6 steps 11, 12
Result	Pass
Finding	N/A
Relevance	N/A

Table 20 – Examination results: OEV paragraph 3.12

Key	3.13
Requirement	Data exchange or storage media, such as USB flash drives, must be removed after the data has been uploaded to the trustworthy components and may only be reused before the data is destroyed if there was no critical data on the trustworthy component before the data was uploaded. Data exchange or storage media must be reformatted and any data on them must be destroyed before they are used with the aid of a component operated in accordance with the requirements for trustworthy components.
Observation	USB sticks are used solely to transfer data in one direction: from the canton to the print office. The encrypted data is copied to the production server, and the USB stick is removed before the data is decrypted. Once the printing process is completed, the data on the stick is securely erased using a dedicated tool.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.5 steps 11, 12

	■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.6 steps 11, 12 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.6 steps 11, 12 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.6 stups 11, 12
Result	Pass
Finding	N/A
Relevance	N/A

Table 21 – Examination results: OEV paragraph 3.13

Key	3.14
Requirement	Logical or physical access to trustworthy components or data carriers containing critical data must be impossible without another person becoming aware of it, for example by having to assist in granting access (strict two-person principle).
Observation	At least two persons are involved in each step of the printing process involving access to trustworthy components or data carriers. ■ One person holds the encrypted data, and another one has the decryption password or the smartcard containing the decryption key. ■ The key of the safe where the USB stick containing the encrypted data is held by one person, and the safe's passcode is known by another person. ■ The password used to access the Output Management System (OMS) server is split in two halves, held by two different persons. At the end of the process all critical data is deleted. The print office provides a checklist of operations performed on the trustworthy components, which is signed by the persons in charge and transmitted to the cantons.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.5 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.6 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.6 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.6 ■ BS: E-Voting BS – Checkliste D+V_1.2 ■ GR: GR_ChecklisteE-Voting_V1.1 ■ SG: Checkliste DV E-Voting St.Gallen_V1.3 ■ TG: Checklist not available yet (first collaboration planned in January 2026)
Result	Pass
Finding	N/A
Relevance	N/A

Table 22 – Examination results: OEV paragraph 3.14

Key	3.17

Requirement	Trustworthy components may perform only the intended operations.
Observation	The printing operations are performed using a dedicated physical server that hosts only the pieces of software necessary for that specific purpose. The server is disconnected from the corporate network and connected to the printer only to generate the e-voting polling cards.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §3.1 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §3.1 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §3.1 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §3.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 23 – Examination results: OEV paragraph 3.17

Key	3.19
Requirement	All procedures for dealing with trustworthy components must be documented in writing and in a manner that is easily understood by the persons concerned.
Observation	The steps for setup, update and operation of the components, as well as for the secure deletion of the data they process are documented in the checklist that is signed by the persons performing the operations.
Evidence	■ BS: E-Voting BS – Checkliste D+V_1.2 ■ GR: GR_ChecklisteE-Voting_V1.1 ■ SG: Checkliste DV E-Voting St.Gallen_V1.3 ■ TG: Checklist not available yet (first collaboration planned in January 2026)
Result	Pass
Finding	N/A
Relevance	N/A

Table 24 – Examination results: OEV paragraph 3.19

Key	3.20
Requirement	Any access to and use of a trusted component or data carrier containing critical data must be logged.
Observation	Each step of the printing process is signed off on a checklist.
Evidence	■ BS: E-Voting BS – Checkliste D+V_1.2 ■ GR: GR_ChecklisteE-Voting_V1.1 ■ SG: Checkliste DV E-Voting St.Gallen_V1.3 ■ TG: Checklist not available yet (first collaboration planned in January 2026)
Result	Pass

Finding	N/A
Relevance	N/A

Table 25 – Examination results: OEV paragraph 3.20

Requirements for printing offices

Key	7.1
Requirement	The printing data used to produce the polling cards are transmitted encrypted and signed. Alternatively, a data carrier containing this data may be delivered in person. In this case, the data carrier must be transported and delivered to the printing office by two persons, who must both stay with the data carrier until it is delivered.
Observation	The encrypted and signed data is transmitted through a portal (cantonal SharePoint platform for the canton of Basel-Stadt and Graubünden, SG Connect for the canton of St Gallen, TG Connect for the canton of Thurgau). In Basel-Stadt, Graubünden and Thurgau, the password for decryption is transmitted via the secure messaging application *Threema*. In St Gallen, the data is encrypted using an asymmetric encryption mechanism embedded into the application used to create the polling card (*VOTING Stimmunterlagen*) and can be decrypted with the private key stored on a smartcard at the print office.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.2 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.3 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.3 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.3
Result	Pass
Finding	N/A
Relevance	N/A

Table 26 – Examination results: OEV paragraph 7.1

Key	7.2
Requirement	The encryption must meet the requirements of eCH standard 0014, Chapter 7.5. If encryption is symmetric, the secret decryption key is sent to the persons responsible at the printing office via a secure secondary channel.
Observation	The eCH standard 0014, § 7.5 lists the recommended cryptographic algorithms to be used by Swiss e-government applications. The cantons of Basel-Stadt and Graubünden encrypt the print data with AES-128 (using the AxCrypt tool). The encryption password is transmitted via the *Threema* secure messaging application. When the next version of the Voting Card Printing Service (VCPS) tool is released (i.e. v3.1), AxCrypt will be replaced by a new tool provided by the Post: File-Cryptor, which relies on AES-256.

Evidence	The canton of St Gallen uses an asymmetric algorithm (RSASSA-PSS algorithm with SHA-256 hash and 3072-bit key length) to encrypt the print data and therefore does not need to transmit any password. ■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.2 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.3 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.3 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.3 ■ Druckerei - PDF Stimmrechtsausweise entschlüsseln und Signatur verifizieren - R1.4 und VCPS 3.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 27 – Examination results: OEV paragraph 7.2

Key	7.3
Requirement	The person responsible at the printing office who receives the data carrier must sign an acknowledgement of receipt.
Observation	Abraxas does not receive the data on a data carrier.
Evidence	N/A
Result	N/A
Finding	N/A
Relevance	N/A

Table 28 – Examination results: OEV paragraph 7.3

Key	7.4
Requirement	For the data carrier containing the print data, the component on which the critical data is decrypted and all components that process the critical data, the provisions for the print component as set out in Number 3 apply.
Observation	The data is decrypted with the offline E-Voting-Server, which is the print component of this print office, and therefore subject to the provisions set out in Number 3. All the components involved in e-voting are subject to the same provisions.
Evidence	■ See 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14, 3.17, 3.19, 3.20 ■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.4 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.5 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.5 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.5

Result	Pass
Finding	N/A
Relevance	N/A

Table 29 – Examination results: OEV paragraph 7.4

Key	7.5
Requirement	The persons responsible at the print office carry out a material quantity check.
Observation	The printers compare the number of documents specified in the original data with the number of documents printed and put in envelopes. A datamatrix code is inserted into the original PDF files and makes it possible to track any losses at each processing step.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.10 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.12 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.12 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.12
Result	Pass
Finding	N/A
Relevance	N/A

Table 30 – Examination results: OEV paragraph 7.5

Key	7.6
Requirement	After printing the polling cards, the print office must destroy the data received.
Observation	The print data is kept encrypted in a safe (see §3.12) until the cantons provide a written confirmation that it may be destroyed. This occurs once the printed material has been delivered and accepted by the cantons.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.5 steps 11, 12 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.6 steps 11, 12 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.6 steps 11, 12 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.6 steps 11, 12
Result	Pass
Finding	N/A
Relevance	N/A

Table 31 – Examination results: OEV paragraph 7.6

Key	7.7
Requirement	If the print office also carries out the packaging and dispatch of the polling cards, these must be packaged together with the voting papers immediately after printing.
Observation	Abraxas does not systematically package the polling cards immediately after printing. When immediate packaging is not possible, the rewound paper rolls from the continuous feed printing process are stored in a locked metal cage featuring a dual-lock mechanism to enforce the four-eye principle. The outer part of the roll consists of 4 to 5 wound layers of white, unprinted paper in order to preserve data confidentiality.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.7 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.9 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.9 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.9 ■ Troax Lagerbox für eVoting_Sicherheitskäfig ■ Sichere Zwischenlagerung bedruckter eVoting-SRA
Result	Partially fail
Finding	The Abraxas print office does not guarantee systematic packaging of the polling cards immediately after printing.
Relevance	N/A

Table 32 – Examination results: OEV paragraph 7.7

Key	7.8
Requirement	The channel between the printing office and the voters may only be considered trustworthy if the bodies responsible under cantonal law deliver the packaged voting papers to the voters by post or ensure that it is handed over in person.
Observation	The voting papers are picked by the postal service.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.8 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.10 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.10 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.10
Result	Pass
Finding	N/A
Relevance	N/A

Table 33 – Examination results: OEV paragraph 7.8

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

Key	14.9
Requirement	All parts of the voting system must be regularly updated in a predetermined and documented process in order to eliminate weaknesses that have become known.
Observation	The parts of the voting system supported by Abraxas include: ■ A physical server (Windows server OS) running two virtual machines ● 1 x Suse Linux / PRISMA print server ● 1 x Windows / DOMTRAC OMS server ■ A Canon ColorStream 3700z printer managed by the print server, thus not receiving direct patches The update process is documented, and related activities are tracked through the company's change management process. Patching is performed prior to each ballot. As the physical server is not connected to the corporate network, the applied patching frequency seems aligned with the risk profile of the system.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §3.2 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §3.2 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §3.2 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §3.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 34 – Examination results: OEV paragraph 14.9

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 documentation contains a list of the print office's employees involved in the generation of voting cards as well as their respective role.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.11 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.2 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.2 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.2
Result	Pass

Finding	N/A
Relevance	N/A

Table 35 – Examination results: OEV paragraph 18.1

Key	18.2
Requirement	The initial configuration of the infrastructure, whether with regard to hardware, software or access rights, and any modification must be approved beforehand.
Observation	Access control and change management are part of the Abraxas ISO 27001 certification's scope, which implies that the allocation of access rights and any modification in the configuration of systems is subject to approval. The document detailing the configuration of the infrastructure and the access control model based upon the 4-eye principle is signed both by the canton and the print office.
Evidence	■ Anwendbarkeitserklärung ISO27001:2022 §A5.15, A8.32 ■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9
Result	Pass
Finding	N/A
Relevance	N/A

Table 36 – Examination results: OEV paragraph 18.2

Key	18.3
Requirement	The risks in connection with third parties (contractors such as suppliers and service providers) must be identified and if necessary reduced by means of suitable contractual agreements. Compliance with the agreements must be appropriately monitored and reviewed throughout their term.
Observation	Abraxas carries out a risk analysis of its suppliers involved in e-voting (i.e. Canon, Docucom). An extract is provided in the documentation. Information security in supplier relationships is part of the Abraxas ISO 27001 certification's scope. This implies that risks identified must be mitigated by suitable contractual agreements.
Evidence	■ eVoting_Risiken-Beurteilung und -Handhabung (Screenshot) ■ Anwendbarkeitserklärung ISO27001:2022 §A5.19-A5.22
Result	Pass
Finding	N/A
Relevance	N/A

Table 37 – Examination results: OEV paragraph 18.4

Management of intangible and tangible resources

Key	19.1
Requirement	All intangible and tangible resources in the sense of the term asset in the standard ISO/IEC 27001, 2013, Information technology - Security techniques - Information security management systems - Requirements , relevant in the context of electronic voting (organisation as a whole, in particular the organisational processes and the information processed in these processes, data carriers, facilities for processing information of the infrastructure and premises of the infrastructure) are recorded in an inventory. A list must be kept of human resources. The inventory and human resources list must be kept up to date. Each intangible and tangible resource is assigned a person who takes responsibility for it.
Observation	Asset inventory is part of the Abraxas ISO 27001 certification's scope. Moreover, the company maintains a list of the e-voting infrastructure components and their respective owners.
Evidence	■ Anwendbarkeitserklärung ISO27001:2022 §A5.9 ■ eVoting-Komponenten_Owner_V1.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 38 – Examination results: OEV paragraph 19.1

Key	19.2
Requirement	The acceptable use of intangible and tangible resources must be defined.
Observation	Abraxas' security policy describes the acceptable use of information and resources. Acceptable use of assets is part of the Abraxas ISO 27001 certification's scope.
Evidence	■ Anwendbarkeitserklärung ISO27001:2022 §A5.10 ■ Policy Informationssicherheit (PIS) v6.19 §5, 6, 7
Result	Pass
Finding	N/A
Relevance	N/A

Table 39 – Examination results: OEV paragraph 19.2

Key	19.3
Requirement	Classification guidelines for information must be issued and communicated.
Observation	Classification of information is part of the Abraxas ISO 27001 certification scope. Abraxas maintains a specific policy on this topic. Being customer data, the print data (i.e., the polling cards) is subject to the *strictly confidential* (streng vertraulich) classification.
Evidence	■ Anwendbarkeitserklärung ISO27001:2022 §A5.12 ■ Policy Klassifizierung von Informationen v12.1 §6
Result	Pass
Finding	N/A

Relevance	N/A

Table 40 – Examination results: OEV paragraph 19.3

Key	19.4
Requirement	Procedures must be devised for the labelling and handling of information.
Observation	Labelling and handling of information are part of the Abraxas ISO 27001 certification scope. The classification policy also specifies how to label and handle information.
Evidence	■ Anwendbarkeitserklärung ISO27001:2022 §A5.13 ■ Policy Informationssicherheit (PIS) v6.19 §5 ■ Policy Klassifizierung von Informationen v12.1 §7
Result	Pass
Finding	N/A
Relevance	N/A

Table 41 – 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	Personnel security is part of the Abraxas ISO 27001 certification scope. The company's personnel undergo a security check when hired and every two years thereafter.
Evidence	■ Anwendbarkeitserklärung ISO27001:2022 §A6 ■ Policy Informationssicherheit (PIS) v6.19 §4 ■ Policy Personen-Sicherheitsprüfung (PSP) v4.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 42 – Examination results: OEV paragraph 20.1

Key	20.2
Requirement	Heads of human resources must accept full responsibility for guaranteeing the trustworthiness of human resources.
Observation	Screening is part of the Abraxas ISO 27001 certification scope. A specific policy on background checks describes how the human resources carry out regular background checks to assert the trustworthiness of human resources.
Evidence	■ Anwendbarkeitserklärung ISO27001:2022 §A6.1 ■ Policy Personen-Sicherheitsprüfung (PSP) v4.1

Result	Pass
Finding	N/A
Relevance	N/A

Table 43 – Examination results: OEV paragraph 20.2

Key	20.3
Requirement	All human resources must be acutely aware of the significance of information security. To this end, an education and training programme that is tailored to the tasks concerned must be devised and operated.
Observation	Information Security Awareness, Education & Training are part of the Abraxas ISO 27001 certification's scope. The company relies on an online training system to regularly educate human resources about information security. Content related to information security is also regularly published on the corporate Intranet. A report detailing the available training modules is issued on a regular basis.
Evidence	■ Anwendbarkeitserklärung ISO27001:2022 §A6.3 ■ Reporting Management-Systeme 2024.11
Result	Pass
Finding	N/A
Relevance	N/A

Table 44 – 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	Physical security perimeter is part of the Abraxas ISO 27001 certification scope. The perimeter for the printing and packaging activities is considered as a protected zone, subject to reinforced security controls.
Evidence	■ Anwendbarkeitserklärung ISO27001:2022 §A7.1 ■ Policy Physische Sicherheit v.17 ■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.1 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.1 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.1 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 45 – 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	Physical security perimeter is part of the Abraxas ISO 27001 certification scope. The security zones are described in the physical security policy. The security controls applying to the perimeter dedicated to the printing and packaging activities are described in the documentation.
Evidence	■ Anwendbarkeitserklärung ISO27001:2022 §A7.2, A7.3, A7.4 ■ Policy Physische Sicherheit v.17 ■ Policy Zutrittskontrolle v4.0 ■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.1 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.1 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.1 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 46 – 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	All domains related to the security of devices (e.g., acceptable use of assets, access control, physical security, operations security, etc.) are part of the Abraxas ISO 27001 certification scope. The devices used in the context of e-voting do not leave Abraxas' premises. The acceptable use of devices is specified in the security policy.
Evidence	■ Anwendbarkeitserklärung ISO27001:2022 §A5.10, A7.8 ■ Policy Physische Sicherheit v.17 ■ Policy Zutrittskontrolle v4.0 ■ Policy Informationssicherheit v6.19 §7
Result	Pass
Finding	N/A
Relevance	N/A

Table 47 – Examination results: OEV paragraph 21.3

Key	21.4

Requirement	All data must be processed and in particular stored exclusively in Switzerland.
Observation	All processing activities related to e-voting data performed by Abraxas occur exclusively in Switzerland. The data is stored on local machines or data carriers sited in St. Gallen-Winkeln, SG.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 ■ Visit of the printing facilities
Result	Pass
Finding	N/A
Relevance	N/A

Table 48 – Examination results: OEV paragraph 21.4

Management of communication and operations

Key	22.1
Requirement	Obligations and areas of responsibility must be apportioned so that the risks originating from human resources relating to operations and communications are reduced to residual risks that are compatible with the risk acceptance criteria.
Observation	The documentation includes the list of people involved in e-voting operations as well as their role. The allocation of roles is done in such a way that there are always two people participating to critical steps of the e-voting operations and that the people in a role have the necessary competence.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.11 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.2 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.2 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 49 – Examination results: OEV paragraph 22.1

Key	22.2
Requirement	Appropriate measures must be taken to protect against malware.
Observation	Controls against malware are part of the Abraxas ISO 27001 certification scope. The security policy also mentions that Abraxas provides an infrastructure that protects against malware.

Evidence	The company uses dedicated equipment (server, USB stick) for e-voting operations, which reduces the risk of malware infection. ■ Anwendbarkeitserklärung ISO27001:2022 §A8.7 ■ Policy Informationssicherheit v6.19 §7.6.1, 7.6.2, 7.7.1, 7.7.2
Result	Pass
Finding	N/A
Relevance	N/A

Table 50 – 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 documentation details the emergency scenarios considered by Abraxas with regards to the information processing facilities related to e-voting. It states that the printing data is stored on the cantons' servers and can be retrieved from those servers in case of loss or disruption. The documentation also declares that the customer is responsible for the backup of e-voting data. Backup is part of the Abraxas ISO 27001 certification scope. The control requires to perform data restore tests on a regular basis to check that backups are functioning correctly.
Evidence	■ Anwendbarkeitserklärung ISO27001:2022 §A8.13 ■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §4.1.1 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §4.1.1 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §4.1.1 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §4.1.1
Result	Pass
Finding	N/A
Relevance	N/A

Table 51 – Examination results: OEV paragraph 22.3

Key	22.4
Requirement	Appropriate measures must be defined and implemented to protect the network from the threats listed in the risk assessment in accordance with Article 4 and in connection with Number 13 and for the security of network services.
Observation	Except the machine used for downloading the encrypted data, none of the machines used for producing the voting material is connected to Internet. The e-voting print server is disconnected from the corporate network and only connected to the printer to generate the polling cards.

Evidence	The zone plan describes how the different network zones are interconnected and isolated with firewalls. Communications security part of the Abraxas ISO 27001 certification scope.
	■ Anwendbarkeitserklärung ISO27001:2022 §A8.20 ■ Netzwerk-Layout ABX Druckerstrasse SG-WKL v1.0
Result	Pass
Finding	N/A
Relevance	N/A

Table 52 – Examination results: OEV paragraph 22.4

Key	22.5
Requirement	The procedures for using removable data carriers and for disposing of data carriers must be regulated in detail.
Observation	The removable data carriers are explicitly mentioned in the documents describing the printing process. At the end of the process, they are either shredded or securely erased.
Evidence	■ BS: E-Voting BS - Prozessbeschreibung Druck und Versand_Abraxas - V1.1 §2.5 step 12 ■ GR: Ablaufbeschreibung DV E-Voting Graubünden inkl. Notfall-Backupszenarien_V1.1 §2.6 step 12 ■ SG: Ablaufbeschreibung DV E-Voting St.Gallen inkl. Notfall-Backupszenarien_V1.1 §2.6 step 12 ■ TG: Ablaufbeschreibung DV E-Voting Thurgau inkl. Notfall-Backupszenarien_V0.9 §2.6 step 12
Result	Pass
Finding	N/A
Relevance	N/A

Table 53 – Examination results: OEV paragraph 22.5

5 Summary of findings and recommendations

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

Key	7.7
Requirement	If the print office also carries out the packaging and dispatch of the polling cards, these must be packaged together with the voting papers immediately after printing.
Finding	The Abraxas print office does not guarantee systematic packaging of the polling cards immediately after printing.
Recommendation	In the auditors' assessment, the secured facility implemented by Abraxas for the temporary storage of printed materials, in cases where immediate insertion is not feasible, provides an adequate mitigation of the associated security risks.

6 References

[1] "Swiss Citizens should be able to vote electronically," Administration numérique suisse, [Online]. Available: https://www.digital-public-services-switzerland.ch/en/implementation/egovernment-implementation-plan/redesigning-evoting. [Accessed 22 May 2024].

[2] "Redesign and relaunch of trials - Final report of the Steering Comittee Vote électronique (SC VE)," Swiss Federal Chancellery, Political Rights Section, 30 November 2020. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/Final%20report%20SC%20VE_November%202020.pdf.download.pdf/Final%20report%20SC%20VE_November%202020.pdf. [Accessed 22 May 2024].

[3] "Partial revision of the Ordinance on Political Rights and total revision of the Federal Chancellery Ordinance on Electronic Voting (Redesign of Trials)," Swiss Federal Chancellery, Political Rights Section, 28 April 2021. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/Explanatory%20report%20for%20consultation%202021.pdf.download.pdf/Explanatory%20report%20for%20consultation%202021.pdf. [Accessed 22 May 2024].

[4] "Federal Chancellery ordinance on electronic voting (OEV)," Swiss Federal Chancellery, 21 April 2021. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/OEV_draft%20for%20consultation%202021.pdf.download.pdf/OEV_draft%20for%20consultation%202021.pdf. [Accessed 22 May 2024].

[5] "Audit concept v1.3 for examining Swiss Internet voting systems," Federal Chancellery (FCh), Political Rights Section, 18 May 2021. [Online]. Available: https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Audit%20concept,%2018.05.2021.pdf.download.pdf/Audit%20concept,%2018.05.2021.pdf. [Accessed 22 May 2024].

[6] "Ordinance on Political Rights (PoRo). section 6a: Electronic Voting Trials," Swiss Federal Chancellery, [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/PoRO_Section%206a%20on%20Electronic%20Voting%20Trials.pdf.download.pdf/PoRO_Section%206a%20on%20Electronic%20Voting%20Trials.pdf. [Accessed 22 May 2024].

[7] "Federal Chancellery Ordinance on Electronic Voting (OEV)," Swiss Federal Chancellery, 25 May 2022. [Online]. Available: https://www.fedlex.admin.ch/eli/cc/2022/336/en. [Accessed 22 May 2024].

[8] P. O. /. S. Adamiste, “Examination of the Swiss Internet voting system, version 1.0 / Audit scope: Infrastructure and operations (3) - Measures of the Abraxas print office,” SCRT SA, 29 November 2022. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_Reports_March2023/Scope%203%20(Abraxas)%20Final%20Report%20SCRT%2029.11.2022.pdf.download.pdf/Scope%203%20(Abraxas)%20Final%20Report%20SCRT%2029.11.2022.pdf. [Accessed 17 March 2025].

[9] P. O. /. S. Adamiste, “Examiniation of the Swiss Internet voting system, version 1.0 / Audit scope: Infrasctucture and operations (3) - Measures of the Baumer print office,” SCRT SA, 29 November 2022. [Online]. Available: https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_Reports_March2023/Scope%203%20(Baumer)%20Final%20Report%20SCRT%2029.11.2022.pdf.download.pdf/Scope%203%20(Baumer)%20Final%20Report%20SCRT%2029.11.2022.pdf. [Accessed 17 March 2025].

[10] “Audit concept v1.5 for examining Swiss internet voting systems,” Federal Chancellery (FCh), Political Rights Section, 15 September 2022. [Online]. Available: https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Vote--lectronique/Audit%20concept%20v1.5.pdf.download.pdf/Audit%20concept%20v1.5.pdf. [Accessed 22 May 2024].

[11] “Audit concept v1.6 for examining Swiss Internet voting systems,” Federal Chancellery (FCh), Political Rights Section, 7 February 2025. [Online].