

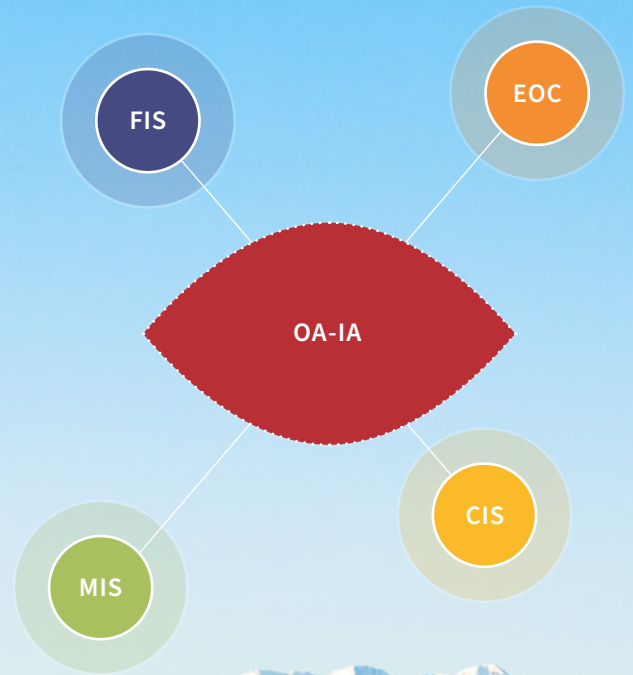


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Independent Oversight Authority
for Intelligence Activities

Annual Report 2022

of the Independent Oversight Authority
for Intelligence Activities OA-IA



1. Summary

The Independent Oversight Authority for Intelligence Activities (OA-IA) began its work in summer 2017, giving it five years of experience to build from. The 2023 audit plan was optimised accordingly and new approaches adopted. For example, the OA-IA has planned an audit to check the controlling procedures used to monitor implementation of its recommendations.

In 2022, the OA-IA also welcomed a new director and three new staff members. This means that 40% of our staff are new to the organisation and have only just begun their supervisory work.

From a technical standpoint, two audits proved particularly challenging for the OA-IA. One was an audit dealing with personnel issues within the Federal Intelligence Service (FIS) ('22-14 Recruiting-, support and leaving process'). This audit was complex for several reasons: the large number of interviews conducted; analysis of the input given in these interviews; and a transformation project launched by the FIS Director, which also had to be taken into account in our reporting. The second challenging audit was Audit '22-18 Data collection by Cyber¹ FIS', which proved to be much more complex than expected as a result of current events and associated reporting on these events.

In 2022, the OA-IA set out to conduct fifteen planned audits for 2022 and two audits carried over from the 2021 audit period. Over the course of the year, it added three additional audits. In the year under review, all audit procedures of a total of 16 audits were performed. The final report on seven of these audits was drafted and sent to the Federal Department of Defence, Civil Protection and Sport (DDPS). For seven other audits, the report is still being drafted and will be formally completed in the first quarter of 2023. Additional audit activities are planned for three audits in 2023.

In the case of the FIS, the OA-IA conducted five audits (four audits of the cantonal intelligence services of Valais, Thurgau, Zug and Schwyz, plus '21-15 HUMINT'). One audit dealt with the Military Intelligence Service (MIS) and another audit with the Electronic Operations Centre (EOC). The OA-IA audited the MIS regarding sensor control and the EOC regarding business continuity management (BCM) and disaster recovery in IT operations.

¹ Organisational unit specialising in the protection of critical infrastructures against threats from state actors from the internet/cyberspace.

2. Key figures as of 31 December 2022



Staff

1 January 2022	9
31 December 2022	10



Audits

Planned audits	15 (18)
Unannounced audits	0 (0)
Audits conducted	16 (18)

Number of interviews

102 (90)

Budgeted workforce

10

Recommendations

13 (18)



- 2022
- 2021
- 2020

3. Table of contents

1. Summary	2
2. Key figures as of 31 December 2022	3
3. Table of contents	4
4. Personal	5
5. Oversight activities	6
5.1 Audit plan	6
5.2 Audits conducted in 2022	6
5.2.1 Strategy and planning	6
5.2.2 Organisation	7
5.2.3 Cooperation	11
5.2.4 Information gathering	12
5.2.5 Resources	15
5.2.6 Data processing and archiving	18
5.3 Acceptance	20
5.4 Controlling implementation of recommendations	20
6. Insights from the inside	22
6.1 Personnel	22
6.2 Initial and continuing training	22
6.3 Access to official documents and information	22
7. Coordination	24
7.1 National contacts	24
7.2 International contacts	25
8. Appendix	29
8.1 Audit Plan for 2022	29
8.2 Abbreviations	30

4. Personal

“We are never satisfied!”

Prisca Fischer



Prisca Fischer, OA-IA Director

In our work, we care about our country's security and the protection of fundamental rights. As professionals, but also as human beings, we must be able to weigh our choices every day. This is to ensure that everyone acts correctly and that every citizen can trust that their fundamental rights will be respected. If we as employees of the oversight authority were not able to pay as much attention to fundamental rights as to security in our work, we would be in the wrong place. However, it is not enough to recognise and adhere to positive values – it also takes curiosity, determination, courage and foresight.

The work of an oversight authority begins by asking questions, especially about risks. These questions awaken our curiosity and we start an audit, which we can only successfully complete with great determination. This is because we must courageously defend our criticisms and our recommendations so that mistakes are corrected and intelligence activities are always carried out within the legal boundaries. Thanks to foresight, we always start each new audit cycle from scratch, with new questions, which we then in turn approach in a spirit of curiosity, determination and courage.

But even this is not enough.

The intelligence services are under our supervision, but they do not work just to answer our questions. They work day and night in the service of our country's security. They take risks every day, including the risk of making mistakes. This is why our commitment and professionalism are required to ensure that we carry out our audits in the right way, in the right place and at the right time. We have to make sure that intelligence work – at least for us – is not an unknown world full of secrets. For us, everything must be clear and transparent. Every day we strive and educate ourselves so that we can enter this world competently.

Is this sufficient now?

Absolutely not! Day after day, we focus on our questions and on the people who work to ensure Switzerland's security. But we also have a duty to the people who have given us this oversight mandate: the citizens. We must be able to prove that we do our work seriously and competently. After all, we examine intelligence activities on behalf of every person in this country who cannot do it themselves. We want you, as a citizen, to read our activity report and see for yourself that we are never satisfied and do not let problems stop us. As you read this report, feel free to send us your feedback and questions.

As the new director of the oversight authority, I work for each and every one of you. We all do.

Prisca Fischer, OA-IA Director

5. Oversight activities

The OA-IA only provides detailed information on selected audits in its annual report. For each completed audit, it publishes a summary of the results on its website.²



5.1 Audit plan

The OA-IA performs risk-oriented audits in the following audit areas:

- Strategy and planning
- Organisation
- Cooperation
- Information gathering
- Resources
- Data processing and archiving

In total, the OA-IA worked on 19 audits. Planned were 15 audits for the year 2022. Since the topic of HUMINT had already been covered in 2021, the OA-IA decided not to conduct Audit '22-9 Human Intelligence (HUMINT)' again in 2022 and postponed this audit to 2023. It also conducted two audits from the year 2021 and three unplanned audits. The OA-IA therefore worked on 19 audits in 2022 and performed all audit procedures of a total of 16 audits. The reporting of seven audits was also completed in 2022, with a further six audits being reported in the first quarter of 2023.

5.2 Audits conducted in 2022

5.2.1 Strategy and planning

In the area of 'Strategy and Planning' the OA-IA checks issues that relate to the short-, medium- or long-term strategic planning of Swiss intelligence agencies and their objectives. The following audit was planned for the year 2022:

- **22-1 Anticipation and early detection (FIS)**

22-1 Anticipation and early detection (FIS)

The anticipation and early detection of relevant threats, strategic developments and corresponding opportunities are vitally important in security policy. But what exactly do these activities entail? Early detection helps to identify and understand a threat. This can be new or result from a change in the situation. Once a given circumstance has been detected, the next step is to take action to influence the development of a situation. This action is essential: the aim is to become an agent of change by planning and taking measures today that will allow us to prepare for a possible change in the future.

“The OA-IA worked on 19 audits in 2022 and performed all audit procedures of a total of 16 audits.”

The FIS plays an important role in the anticipation and early detection of relevant threats. According to the foreword given by the head of DDPS in the 'Security Switzerland 2021' situation report, improved early detection should enable more targeted action to counter cyber threats, disinformation and influence activities directed against Switzerland and also diffuse hybrid threats. The latter occur in modern conflict scenarios when conventional military operations are combined with economic pressure, computer attacks or propaganda in media and social networks. These phenomena are becoming increasingly important from a security policy standpoint and require greater attention.

Information gathering and processing facilitate the early detection and prevention of threats to internal and external security. Social and technical advances as well as the increasingly global nature of today's threats require the FIS to improve its ability to detect these threats earlier and to respond to them more quickly and effectively.

The amount of publicly accessible information available in real time via modern information technologies does not make intelligence services superfluous. They still need to: sift through and evaluate countless reports; supplement and verify information using data that is not publicly accessible; condense raw data in a way that enables timely situation analyses. This is the only way to ensure that the Federal Council has a sound basis for strategic decisions. The OA-IA included this audit in its audit plan in order to determine whether and how the FIS fulfils this important task. The audit report was being finalised at the time this annual report was being written. Once the final report has been completed and submitted to the DDPS, the OA-IA will publish the audit summary on its website.

5.2.2 Organisation

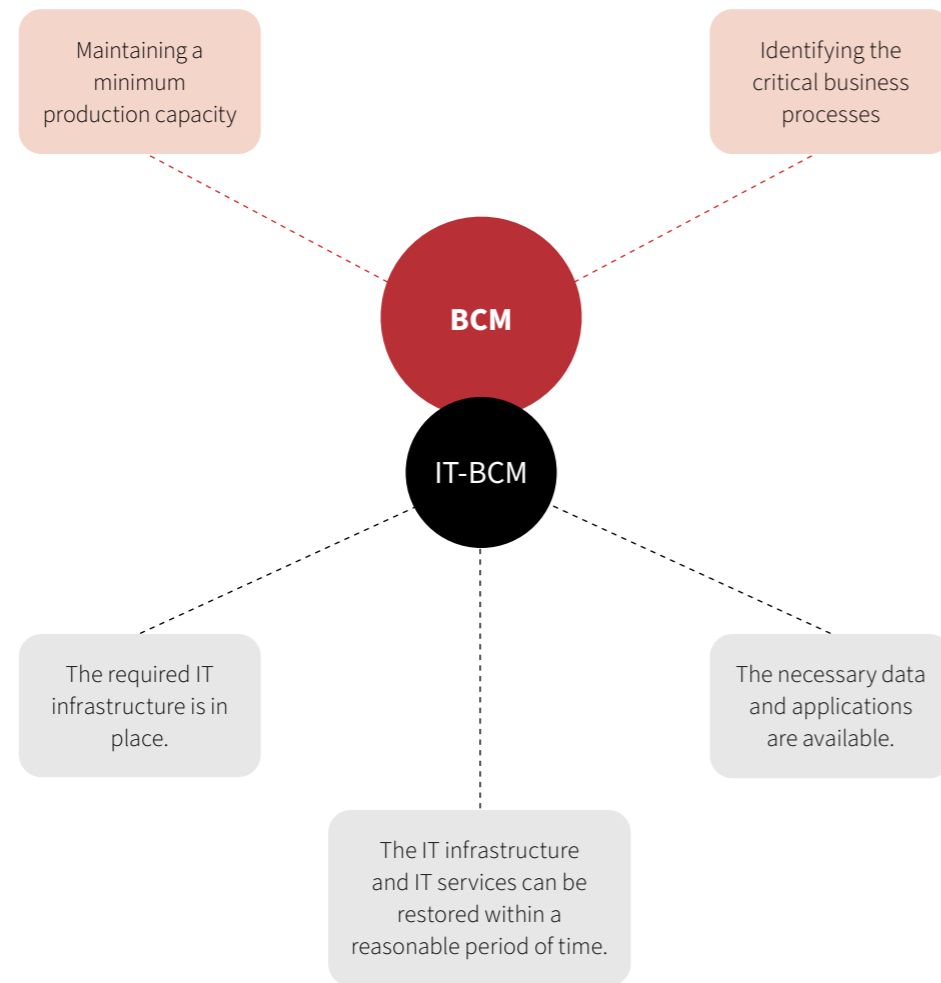
In the area of 'Organisation' the OA-IA checks the suitability of the structure and processes of the intelligence services and asks whether they enable the authorities to carry out their legal mandate in a lawful, expedient and effective manner. The OA-IA conducted the following audits in this area in 2022:

- **22-2 Business Continuity Management and Disaster Recoveries in IT Operations (EOC)**

22-2 Business Continuity Management and Disaster Recoveries in IT Operations (EOC)

Unforeseen events such as damage to cables caused by construction work, natural disasters such as floods, or direct attacks on the information technology infrastructure affect not only private individuals, but also companies and state institutions. Business continuity management (BCM) involves analysing and managing the risks that such threats pose for the entire organisation. Given the heavy reliance of business operations on information technology, the existence of a fail-safe IT infrastructure is essential for the survival of an organisation. In this sense, IT-BCM provides technical support for business continuity management and ensures that the IT infrastructure and corresponding IT services can withstand a disaster and/or be restored within a reasonable timeframe and in accordance with established priorities. BCM is therefore concerned with maintaining a minimum production capacity in any situation and identifying the critical business processes needed for this purpose. IT-BCM, on the other hand, ensures a certain redundancy of the required IT infrastructure, data and applications. It also enables service to be restored within a reasonable period of time after disruptions.

² <https://www.ab-nd.admin.ch/de/pruefplan-und-pruefberichte.html>.



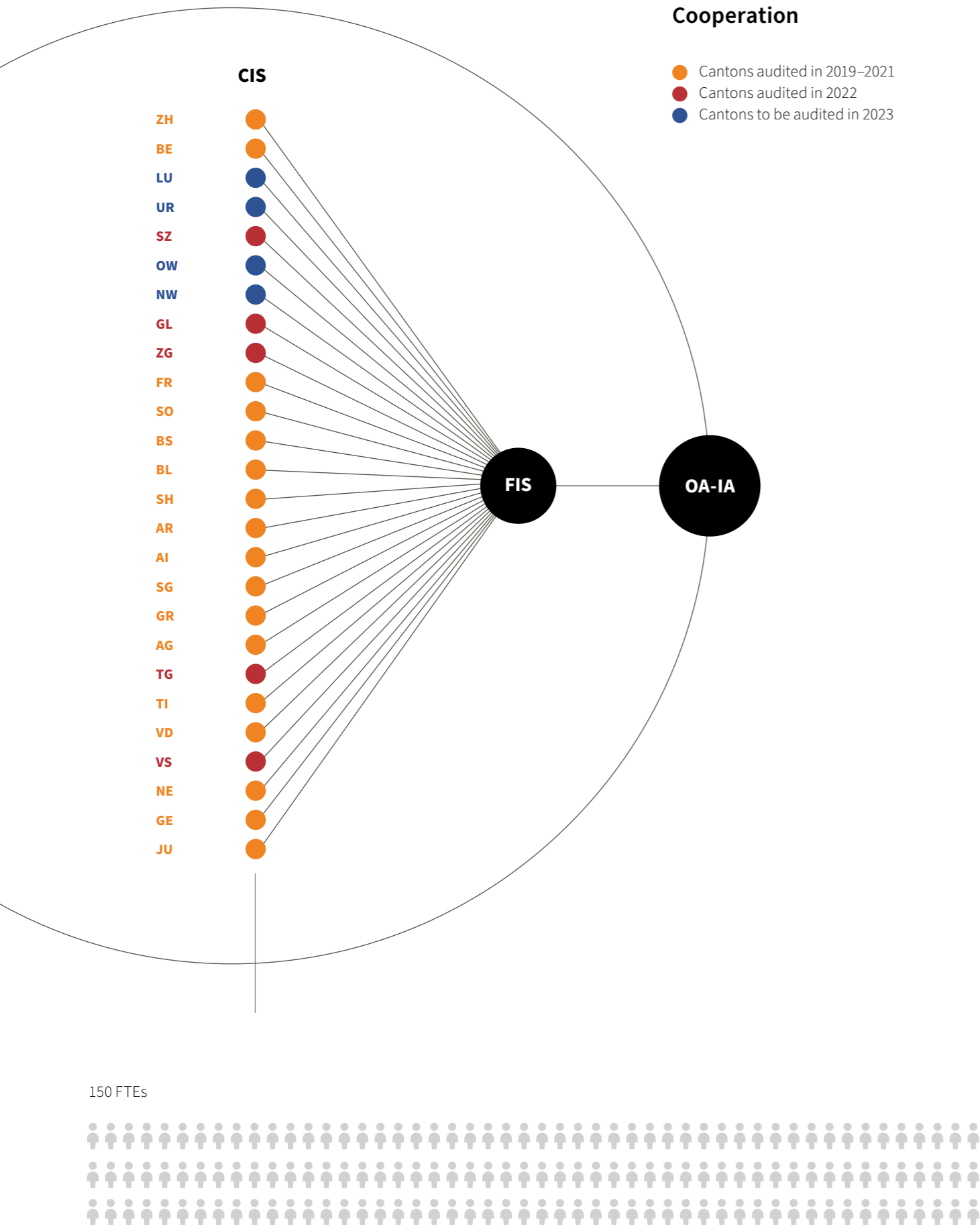
The primary task of intelligence services is to obtain and process data in order to gather information that is needed to safeguard our country's security interests. Like all other organisations whose business model is based on information processing, they are particularly dependent on IT systems that remain highly available. Therefore, the above-mentioned disasters also affect the business processes of such organisations directly. This is because the loss of information technology directly affects their ability to guarantee critical business processes. For these organisations, BCM and IT-BCM are closely related. This prompted the OA-IA to review the business continuity management of information technology as well as the IT-disaster recovery at the EOC.

The OA-IA noted in its audit that the EOC bases its considerations mainly on internal risk management. In this context, preventing and reducing risks to an acceptable level are just as important as ensuring the recovery of the IT infrastructure after a disaster scenario occurs.

In addition, the EOC is constantly working to optimise its BCM and disaster recovery capabilities in IT operations. This includes the creation and further development of strategies and plans, but also ongoing investments in the IT infrastructure to ensure that back-up and disaster recovery mechanisms remain technologically up-to-date.

Overall, the OA-IA concluded that the EOC is well equipped in the area of BCM and disaster recovery in IT operations.





“In addition to an on-site audit, which includes a technical discussion with the CIS staff in charge and a tour of the premises, the OA-IA also carries random samples of the various information systems.”

5.2.3 Cooperation

The OA-IA checks the level of cooperation between the cantonal intelligence services and national and international authorities. Each year, the OA-IA examines cooperation with selected cantonal intelligence services (CISs). In 2022, it conducted the following audits:

- 22-3 Cantonal Intelligence Service of Valais (CIS/FIS)
- 22-4 Cantonal Intelligence Service of Glarus (CIS/FIS)
- 22-5 Cantonal Intelligence Service of Thurgau (CIS/FIS)
- 22-6 Cantonal Intelligence Service of Zug (CIS/FIS)
- 22-7 Cantonal Intelligence Service of Schwyz (CIS/FIS)

Audits 22-3 to 22-7: Audits of the cantonal intelligence services of Valais, Glarus, Thurgau, Zug and Schwyz (CIS/FIS)

In 2022, the OA-IA audited the intelligence activities of the CIS in the cantons of Valais, Glarus, Thurgau, Zug and Schwyz. Since taking up its oversight activities, the OA-IA has thus audited a total of 22 CISs. The audit of the remaining four CISs³ is scheduled for the 2023 audit period.

To ensure comparability, the OA-IA uses the same procedure to audit all CISs. In addition to an on-site audit, which includes a technical discussion with the CIS staff in charge and a tour of the premises, the OA-IA also carries random samples of the various information systems.

All CIS audits 2022 found that the FIS and the CISs basically cooperate well to very well in all areas of intelligence. The CISs have a good to very good understanding of intelligence tasks and possess the motivation needed to accomplish these tasks. The OA-IA examined an average of five mandates that the FIS had given to the respective CIS from the years 2020 to 2022. It considered aspects such as the purpose of information gathering, the actions taken, the results achieved

and whether or not the CISs met the deadlines set by the FIS. The results of these samples, as well feedback from FIS performance assessments, led the OA-IA to conclude that the audited CISs completed the mandates given to them by the FIS in a lawful manner, on time and provided a level of quality deemed satisfactory by the FIS.

Due to a lack of resources and technical means for data processing, CIS Zug kept unprocessed audio files on an external hard drive for an extended period of time. The OA-IA recommended the FIS to ensure that the CIS comply with the applicable requirements regarding the duration of the retention period of data outside the FIS network. In the future, the FIS quality assurance unit should include verification of data on external data storage media when conducting periodic random samples.

Differences in the way individual CISs operate are particularly visible in small CISs with limited staff numbers. In one CIS, the head did not carry out any intelligence activities and did not have access to FIS information systems. In another CIS, the deputy head only filled in when the head was absent, but was not involved in the day-to-day operations. In both cases, however, these individual forms of organisation had no discernible negative effects on the fulfilment of the mandates given.

The distribution formula used to calculate the amount of compensation that the FIS pays to the CISs remained unchanged until the end of 2022. After that, this formula will be adjusted. The smaller CISs, in particular, which are affected by a possible reduction in compensation, became disgruntled by the proposed changes. The FIS and the Conference of Cantonal Police Commanders of Switzerland (CCPCS) therefore set up a working group to jointly establish the criteria to be met for the next distribution formula. Since their work began only in early 2023, the period of validity of the current distribution formula has been extended until the end of 2023.

³ Lucerne, Nidwalden, Obwalden and Uri

“The FIS is required to choose the information-gathering measure that has the least impact on the fundamental rights of the persons concerned.”

5.2.4 Information gathering

Information gathering is a core task of intelligence services. Various means can be used for this purpose. The OA-IA pays special attention to those that most deeply invade the privacy of the persons concerned.

Each year, a special audit is conducted in the area of HUMINT. Audit ‘21-15 HUMINT’ planned for 2021 could not be fully carried out in the year itself and was only completed in 2022. Therefore, Audit ‘22-9 HUMINT’ scheduled for 2022 was cancelled. The HUMINT area was also covered in 2022 by another audit in the Resources area ‘22-13 Legended financial flows.’⁴

In the area of information gathering, the OA-IA conducted the following audits in 2022:

- 21-15 HUMINT
- 22-8 Operations, operational clarifications and information-gathering measures requiring authorisation (FIS)
- **22-10 Information-gathering measures not requiring authorisation (FIS)**
- **22-11 Information gathering management (FIS)**
- **22-12 Sensor control and selection in military intelligence (MIS)**

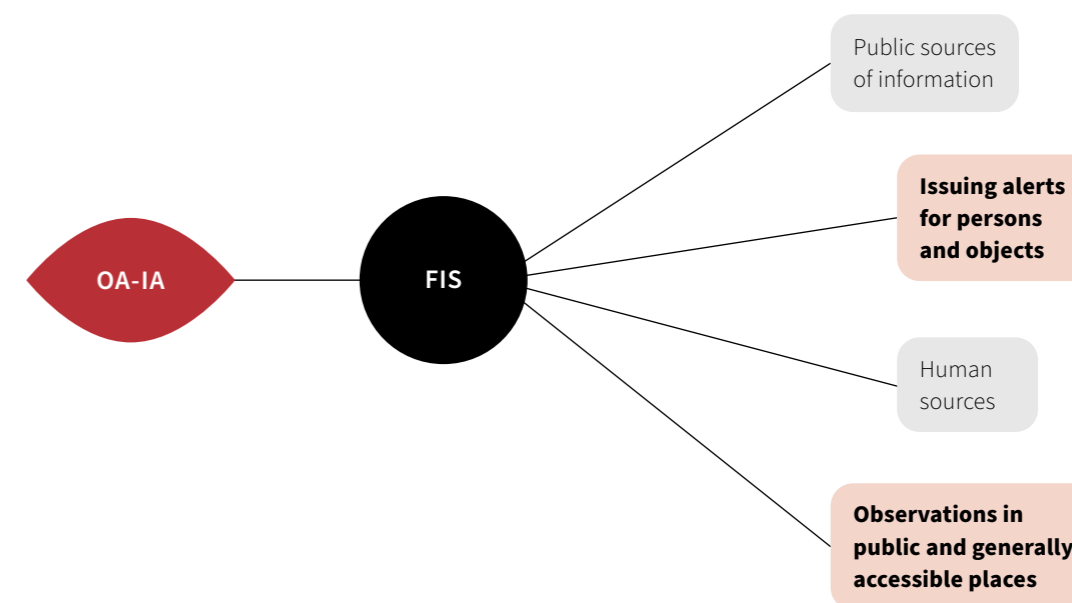
22-10 Information-gathering measures not requiring authorisation (FIS)

In order to fulfil its tasks, the FIS obtains information from publicly and non-publicly accessible information sources.⁵ In each case, the FIS is required to choose the information-gathering measure that has the least impact on the fundamental rights of the persons concerned. The FIS can take certain measures to gather information independently and without having to obtain specific external authorisation. This is because the intensity of interference with fundamen-

tal rights of such measures is relatively low. These measures include gathering information from public sources, carrying out observations in public and generally accessible places, using human sources and issuing alerts regarding individuals and property. The OA-IA mainly focused on observations (e.g. video and audio recordings) in public and generally accessible places (e.g. airports, streets or railway stations) and the use of the computerised police search system (RIPOL), including the national part of the Schengen Information System (N-SIS).

Any observation carried out in public and generally accessible places requires a very careful analysis of the circumstances on site, as the question of whether or not permission for information gathering is required may depend, for example, on the angle of a camera shot. Recording conversations can also be tricky, especially because the criminal law definition of what is and what is not a private discussion makes it difficult to implement measures in real situations. The OA-IA therefore examined all processes used to implement these measures as well as the corresponding technical means used to obtain and process such information.

RIPOL is used by federal and cantonal law enforcement agencies to issue alerts concerning persons and property in Switzerland. The FIS can also issue alerts in RIPOL for persons and vehicles if there are well-founded indications that the person in question poses a concrete threat to the internal and external security of Switzerland, if a vehicle is being used for such a threat, or if establishing the whereabouts of a person or vehicle is necessary to safeguard vital national interests. The N-SIS is used to process the same alerts, but on an international level in the Schengen area. The OA-IA examined the processes leading to the issuance of alerts in RIPOL and the N-SIS. Auditors also checked access authorisations as well as the management and control of data searches from the two systems. To do this, the OA-IA



conducted its audit activities at the FIS and obtained clarifications from the Federal Office of Police (fedpol).

The audit report had not yet been completed at the time this annual report was being drafted. For this reason, no assessment could be made at that time.

22-11 Information gathering management (FIS)

The Information Management Division (IM) is part of the Information Gathering Directorate of the FIS. It performs one of the core tasks of the directorate by coordinating information-gathering assignments. It also provides a continuous overview of the information-gathering activities carried out by the FIS. In this respect, the IM Division serves as the directorate's nerve centre.

In its previous audits, the OA-IA had repeatedly come into contact with the IM Division, but had never reviewed its activities in detail. Therefore, in this audit, the OA-IA examined the following in particular:

- whether the tasks, remits and responsibilities of the IM Division are expedient and effective with regard to fulfilment of the tasks entrusted to FIS under Art. 6 IntelSA;
- whether the IM Division is adequately integrated within the FIS structure;
- whether cooperation with other organisational units within the FIS and with third parties is expedient and effective.

In this audit, the OA-IA reviewed the entire IM Division. Auditors examined actual information gathering management – also referred to as collection management – as well as two other areas.

In its audit, the OA-IA also reviewed the extensive documentation describing the tasks, remit and responsibilities of the IM Division and the areas included. This documentation was comprised of manuals, processes, memos and business management processes.

The OA-IA then checked to see whether the procedures described in the documentation were actually followed. The OA-IA obtained this information from interviews with IM staff and by consulting the FIS file storage system and then randomly reviewing cases handled by the IM staff interviewed.

In order to assess the level of cooperation with other organisational units in the FIS and with third parties, the OA-IA conducted interviews with other FIS employees, for example from the Evaluation Division, whose daily work is directly affected by the activities of the IM Division. Analysts prepare information gathering assignments, which are then reviewed by the IM Division and, if necessary, sent back for additions and/or corrections. Written questions were also sent to external bodies to find out more about their daily cooperation with the IM Division. These bodies included in particular the independent Post and Telecommunications Surveillance Service (PTSS) and the EOC.

⁴ See Section 5.2.5 below.

⁵ Art. 5 of the Federal Act of 25 September 2015 on the Intelligence Service (Intelligence Service Act, IntelSA; SR 121).

“The OA-IA found that MIS sensor control and selection during domestic assistance missions were handled in a lawful, expedient and effective manner.”

It can be stated out, that the auditors were unable to clearly determine who specifically was responsible for information gathering assignments. The OA-IA recommended optimising certain processes. The DDPS has forwarded the two recommendations to the FIS for implementation.

22-12 Sensor control and selection in the Military Intelligence Service (MIS)

This audit mainly dealt with the question of whether sensor control and selection in the MIS take place lawfully, expediently and effectively during missions of the Swiss Armed Forces. In its letter dated 26 November 2021 on the draft 2022 audit plan, the Control Delegation of the Swiss Parliament (CDeI) informed the OA-IA that, for example, the issuing of assignments for radio communications intelligence and the planning of MIS contacts with partner services were long-term undertakings and could not be adapted to new procurement objectives at short notice. Therefore, auditors were told that it did not make sense to analyse sensor control from the standpoint of MIS administrative processes. Instead, it made more sense to examine sensor control within the context of specific missions carried out by the Swiss Armed Forces. The OA-IA took this advice on board in the audit design and focussed its audit activities on selected specific missions of the Swiss Armed Forces at home and abroad.

The OA-IA found that MIS sensor control and selection during domestic assistance missions (specifically the 2022 World Economic Forum Annual Meeting and the 2022 Ukraine Recovery Conference) were handled in a lawful, expedient and effective manner. In addition to the usual audit activities, such as inspecting documents, auditors also visited the MIS operations room and conducted interviews with staff members in the audited unit. All participants in the above-mentioned discussions gave a positive assessment of MIS actions. The OA-IA also took this into account in its assessment.

The OA-IA's audit activities also revealed that the MIS obtains and evaluates information on foreign countries that is significant for the Swiss Armed Forces; auditors confirmed that sensor control and selection was carried out lawfully, expediently and effectively. That said, the MIS is not directly involved in peace building or support missions abroad; thus, the OA-IA could not audit MIS sensor control and selection in these circumstances due to the lack of an auditable object.

5.2.5 Resources

In the area of 'Resources', the OA-IA considers whether the intelligence services are handling resources in an expedient manner and whether intelligence activities are carried out effectively.

In 2022, the OA-IA conducted the following audits relating to 'Resources':

- **22-13 Legended financial flows (FIS)**
- **22-14 Recruiting-, support- and leaving process (FIS)**

22-13 Legended financial flows (FIS)

The FIS conducts most of its information gathering activities covertly. This is essential because if the affected states and actors become aware of these activities, they can take countermeasures. In addition, covert activities protect FIS staff and facilities as well as the human sources working undercover. These are individuals who have exclusive access to information and are willing to give this information to the FIS. Human sources often charge money for their information. The FIS is authorised to provide them with adequate compensation for their activities.⁶ Payments made by the FIS to undercover sources – and thus proof of their work for the FIS – can pose a great risk in the source's country of origin as well as

⁶ Art. 15 para. 2 IntelSA

“Incorrectly executed payments can allow third parties to draw undesired conclusions about FIS staff and facilities as well as about the sources, thereby putting them at risk.”

in their personal environment if their work becomes public. Suspicion of income due to intelligence connections and activities can damage a source professionally, destroy his/her reputation and, depending on the country and environment, put him/her at great risk to life and limb. Therefore, for reasons of self-protection and to protect undercover sources, the FIS must have the means of transferring money that does not reveal the FIS as the original sender.

Since 2018, the OA-IA has conducted annual audits of the HUMINT Division. During these audits, random sampling is used to verify the legality, expediency and effectiveness of source management. Auditors also consider whether the amount paid out to undercover sources is justified on the basis of performance. The present audit, however, dealt exclusively with the path of money and legended financial flows within the FIS.

Incorrectly executed payments can allow third parties to draw undesired conclusions about FIS staff and facilities as well as about the sources, thereby putting them at risk. If these risks were to occur, they would inevitably damage the reputation and credibility of the FIS. There would also be operational effects such as hindering or even preventing information gathering.

In order to assess the legality, expediency and effectiveness of the methods used by the FIS to handle legended financial flows, the OA-IA reviewed the financing of two institutions, six financial infrastructures used to pay undercover sources as well as one case where the FIS and a foreign partner intelligence service jointly managed a source. It also reviewed another case in which the FIS worked with a partner intelligence service to conduct a joint operation.

The audit activities were completed by the end of 2022 and the final audit report was being finalised as this annual report went to press. While the results of the final audit report cannot be anticipated, it can be stated that the FIS uses legal, expedient and effective methods when providing funds to a beneficiary. Nevertheless, the OA-IA intends to submit a recommendation to the DDPS⁷ regarding the completeness of reporting.

22-14 Recruiting-, support- and leaving process (FIS)

There are significant security risks from within intelligence services as their own employees can betray their organisation, steal data or engage in espionage. Therefore, in 2019, the OA-IA conducted an audit of both the MIS and the EOC with the same audit questions as the ones used for Audit 22-14 of the FIS.⁸

In 2019, the OA-IA found that different classification practices regarding personnel security screening (PSS) had been established for the three intelligence services, FIS, MIS and EOC. Under current legislation, there are three different PSS levels: basic security screening, which is required when employees have access to information classified as confidential; enhanced personnel security screening, when the person concerned has access to information classified as secret; and enhanced PSS combined with questioning, when the person has regular access to classified internal and external security information.⁹

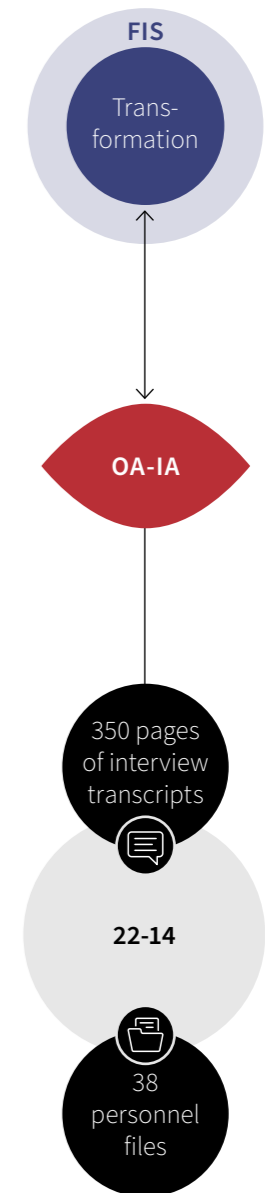
All employees of the three intelligence services must undergo such an audit whenever they start working in the services. This audit is repeated at regular intervals. The OA-IA was unable to understand the different classification rules objectively and logically. It therefore recommended to the head of the DDPS that the classification practice for the three intelligence services be reviewed and, if possible, standardised.

⁷ According to Art. 19 IntelSO
⁸ See 2019 OA-IA Annual Report, p.22 pp.
⁹ Art. 10 to 12 of the Ordinance of 4 March 2011 on Personnel Security Screening (PSSO; SR 120.4)

The new Information Security Act and its implementing regulations provide for only two levels of personnel security screening instead of three. The extent to which classification practices will be standardised after the draft legislation comes into force cannot be assessed at this time.

For Audit 22-14, the OA-IA shifted its focus compared to the two audits mentioned above, focusing instead on the recruiting and support of FIS staff. The poor results from the last staff survey in the Federal Administration and the high staff turnover rates, combined with frequent changes at the top-management level, justified this approach. Less attention was paid to the audit questions regarding deactivation of access to buildings and information systems after staff departure. Auditors also paid little attention to the process of re-initiating regular PSS. This was due to the fact that the OA-IA already checks access processes in its regularly conducted audits of information systems. In addition, the FIS follows the strictest PSS classification practice of all three intelligence services and has established documented processes for this purpose.

Here, the OA-IA wanted to obtain a representative sample through interviews with staff members. For this purpose, it carried out the logistically challenging task of conducting over thirty interviews. Appropriate consideration was given to the gender, age, language composition, selection of members of FIS working groups and hierarchical levels of the staff interviewed. Several FIS employees spontaneously made themselves available for an interview, others asked if they could make additional statements in connection with previously held interviews. The OA-IA did not disclose all the names of the staff interviewed to FIS management. This ensured that they could answer without bias. In the course of the audit, the OA-IA analysed over 350 pages of interview transcripts and carried out random sampling in 38 personnel files.



“When involving telecom service providers, what steps have been taken to ensure that no information is gathered that would require preliminary authorisation?”

Another challenge resulted from the transformation project launched by the FIS Director, who intends to transform the service. The OA-IA will pay special attention to this circumstance in its assessment. The results of the audit cannot yet be conclusively stated in this annual report. The OA-IA plans to complete the audit at the beginning of the second quarter of 2023 and submit a definitive report.

5.2.6 Data processing and archiving

In the area of ‘Data processing and archiving’, the OA-IA verifies the legality of information processing. This is due to the fact that the information processed by intelligence services is highly sensitive and the legal requirements are as extensive as they are complex.

In 2022, the OA-IA conducted the following audits in this area:

- **21-16 Telecommunication services (FIS)**
- 22-15 Open-source intelligence (OSINT) (FIS)
- 22-16 FIS and EOC links to Swiss telecommunication service providers (FIS)
- 22-17 Follow-up 20-19: Archives of the FIS (FIS)
- **22-18 Data collection by Cyber FIS (FIS)**

The activities for Audit ‘22-15 Open-source intelligence (OSINT)’ did not start until the fourth quarter of 2022. The activities for Audit ‘21-16 Telecommunication services’, on the other hand, were completed in 2022, although the report was not yet available by the editorial deadline set for the 2022 annual report. With Audit ‘22-17 Follow-up to 20-19: Archives’, the OA-IA intends to assess the action steps decided by the FIS in the wake of Audit ‘20-19 Archives’. The first audit activities have already been carried out.

21-16 Telecommunication services (FIS)

Social media platforms such as WhatsApp or Telegram are increasingly being used to exchange information with friends and acquaintances. End-to-end encryption is used by these providers to secure the content of communication. The FIS handles requests for access to information on end-to-end encryption applications operated by Swiss telecom providers. It is important to note, however, that these requests do not focus on the content of communication, but rather only on the marginal data¹⁰ that can be used to identify the parties involved in communications.

The FIS has observed an increase in such requests in recent years. For this reason, it centralised the internal processing of such requests. This audit was conducted to ascertain whether centralisation had improved the process.

The OA-IA considered the following questions:

- Is there a valid legal basis for the FIS to directly involve telecom service providers and use the information obtained from them?
- When involving telecom service providers, what steps have been taken to ensure that no information is gathered that would require preliminary authorisation?
- What steps have been taken to ensure that the FIS only receives and processes information relating to the assignment at hand?
- Is the process used for such clarifications expedient?

In addition to interviews, the audit activities focused on a significant number of samples of clarifications processed in the period from 2020 to 2022. Although the audit activities had been completed when this annual report was written, the

¹⁰ Marginal data are data that contain information about the use of electronic infrastructures. They document, for example, which telephone connection, which e-mail sender or which IPT address communicated when, for how long and with whom.

“Analysis of the final reports from the internal and administrative investigations led the OA-IA to conclude that still not all relevant questions had been answered.”

results are not yet ready. The OA-IA plans to submit the final audit report at the start of the second quarter of 2023. A summary of the answers to the audit questions will therefore be published online in the usual form.

22-18 Data collection by Cyber FIS (FIS)

From 2015 to 2020, during investigations of suspected cyber attacks, the FIS also obtained information that is subject to telecommunications confidentiality rules. Under IntelSA, these information-gathering measures require authorisation from the Federal Administrative Court. The FIS had not asked the FAC for this authorisation. In addition, it recorded the network traffic of servers used by cyber attackers, also without FAC authorisation.

In May 2021, the FIS Director at the time notified the OA-IA of possible irregularities and informed us that an internal investigation had been launched to examine the processes followed by the Cyber FIS Division. In addition to the internal investigation, the FIS commissioned an external evaluation to obtain a legal opinion. In two anonymous letters, the OA-IA received additional background information on the facts of the case.

The OA-IA closely followed the FIS’s internal investigation. The OA-IA insisted that it be provided with reports and documents if the deadlines agreed with the FIS were not met. Over the course of the investigation, it was ascertained that the Cyber FIS Division had heeded the FIS Director’s instruction to cease and desist with the data collection in question. The FIS’s internal investigation mandate also included the right questions. The final report was written quite critically and made various recommendations, such as ensuring that employees of the Cyber FIS Division received proper training on the legal

aspects associated with their tasks; and the importance of restructuring the Cyber FIS Division. The latter resulted in the Cyber FIS Division being assigned to the Evaluation Division.

In the same context, the DDPS launched an administrative investigation in January 2022 which should have clarified the open questions from the internal investigation. At the same time, other measures, such as the filing of a criminal complaint, were supposed to be considered.

Analysis of the final reports from the internal and administrative investigations led the OA-IA to conclude that still not all relevant questions had been answered. These related in particular to individual aspects, such as legended financial flows, the use of hardware developed and made available by the FIS for data collection, and a possible transfer of data to an external party.

The OA-IA also received additional internal information from the FIS, which prompted it to conduct its own audit activities. In particular, auditors held interviews with affected staff members and supervisors. The OA-IA then transferred the resulting documentation to Audit 22-18. The following audit questions will be examined in this audit:

- Have all the facts enabling assessment of the events at Cyber FIS been fully documented?
- What steps has the FIS taken to ensure that analysis of data traffic obtained from providers takes place in a lawful manner in the future?
- Are the organisational measures and controls taken by the FIS to prevent such incidents in the future appropriate and effective?

Since the audit activities had not been completed at the time this annual report was written, the OA-IA cannot yet make any statements on possible findings or need for action. However, the OA-IA notified the FIS Director and the head of the DDPS in December 2022 that according to an interim finding, an urgent measure formulated by the FIS itself in the internal audit report had not been implemented. The OA-IA noted on this occasion that action needed to be taken before the audit was completed.

5.3 Acceptance

The OA-IA auditors were welcomed by the supervised organisational units in a constructive and professional manner. They were given direct access to the documents and information systems required to carry out their audit tasks. Auditors also had no difficulties reaching interviewees whenever they needed them. Any further questions were answered as quickly as possible.

5.4 Controlling implementation of recommendations

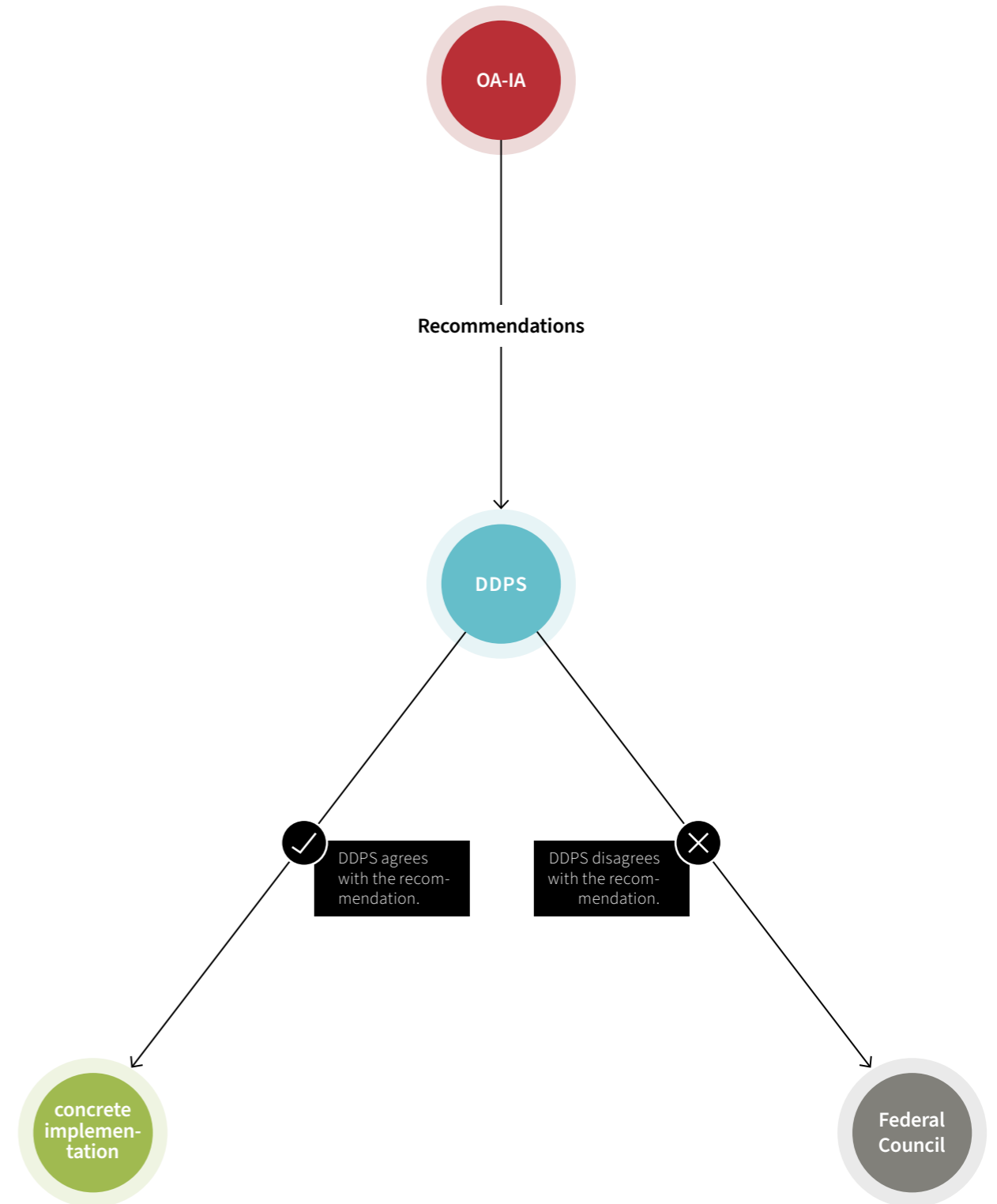
Under IntelSA, the OA-IA can make recommendations on the basis of its audit activities and submit these to the DDPS. The DDPS then ensures that these recommendations are implemented. If the DDPS rejects any OA-IA recommendations, it must submit them to the Federal Council.

The legal bases for intelligence services do not explicitly regulate verification of implementation of recommendations. The OA-IA agreed with the DDPS and the supervised authorities

that the latter would keep the DDPS and the OA-IA informed of progress on implementation of OA-IA recommendations. Moreover, it was agreed that an annual meeting would be held with the supervised services in the presence of the intelligence advisor to the head of the DDPS to discuss pending and implemented recommendations. When the present annual report was published, 19 of the recommendations made by the OA-IA to the FIS and 4 of those made to the MIS were still pending. So far, the supervised services have implemented 150 recommendations since the OA-IA was established.

The OA-IA keeps a record of the recommendations that it issues. As part of the follow-up process, it receives regular updates from the supervised services regarding implementation. As soon as it receives notification that a given recommendation has been implemented, the OA-IA decides whether the implementation described is sufficient or whether the matter needs to be re-examined more closely. This review can either be included in another planned audit or made part of an additional audit. While the number of recommendations made per audit year was high in the past (2019: 63 recommendations), this number has decreased significantly since then (2022: 13). This was partly due to the fact that the OA-IA had heeded the CDeI's criticism that 'too many recommendations would mainly create more red tape and lead to excessive regulation of intelligence services'.¹¹ In addition, the OA-IA consistently pursued the approach of ensuring that its recommendations would provide tangible benefits for the supervision and management of the intelligence services. The result has been fewer, but more targeted and effective recommendations.

¹¹ Annual report of the Control Committee (CC) and the Control Delegation (CDeI) of 25 January 2022, p. 134 (BBl 2022 513)



6. Insights from the inside

“The auditors expanded their knowledge, skills and qualifications through regular initial and continuing training.”

In this chapter, the OA-IA reports on internal matters.

6.1 Personnel

In 2022, the OA-IA – as budgeted – set a target of 10 staff members.¹² After three departures in 2021, the OA-IA hired three new colleagues in 2022. The Director of the OA-IA also left at the end of March 2022. The deputy Director took over as head for three months, until Prisca Fischer was appointed as the new Director on 1 July 2022.

6.2 Initial and continuing training

Continuous development of staff is an important factor ensuring OA-IA success. Its auditors expanded their knowledge, skills and qualifications through regular initial and continuing training. In 2022, for example, they attended relevant events on OSINT, information technology, privacy and future geopolitical developments. The OA-IA also organised in-house training on questioning techniques, counterintelligence, cyber security, security policy, OSINT and surveillance of telecommunications.

6.3 Access to official documents and information

As part of the decentralised Federal Administration, the OA-IA works on behalf of citizens. They have a right to know what the authorities are doing and how they are fulfilling their mandate. As a result, citizens have the right to gain access to information and at the same time the authorities have a duty to provide information.

The Freedom of Information Act¹³ determines the scope and boundaries of passive information. Any person may request access to official documents without having to claim a special interest. The OA-IA did not receive any requests for access to official documents in the reporting year. It answered seven enquiries from media representatives.

¹² 8.6 full-time equivalents shared by ten employees.

¹³ Federal Act of 17 December 2004 on Freedom of Information in the Administration (Freedom of Information Act, FoIA; SR 152.3)



Bridge over the Rhine in Diessenhofen (Thurgau)

7. Coordination

The OA-IA coordinates its activities with those of parliamentary oversight bodies as well as with those of other federal and cantonal oversight bodies.¹⁴ After the pandemic years 2020 and 2021, this interaction intensified again during the reporting year.

7.1 National contacts

Federal Administrative Court (FAC)

During the reporting year, representatives of the FAC and the OA-IA met twice. On 23 March 2022, they discussed the court's rejection and authorisation of information-gathering measures, questions on cable communications intelligence, the upcoming consultation procedure on the revision of the IntelSA and the OA-IA's audit plan for 2022.

On 26 October 2022, both parties also discussed the latest developments in case law on intelligence activities, the new audit plan for 2023 and the corresponding audit reports. They expressed their interest in the bi-annual meetings. The meetings will therefore continue at this rhythm. The head of the OA-IA proposed that the meetings be used to extensively discuss one topic of common interest at a time.

Swiss Federal Audit Office (SFAO)

The SFAO and the OA-IA met on 18 July 2022 and spoke on the phone on 16 November 2022. The OA-IA's 2023 audit plan and other audit topics were discussed.

Post and Telecommunications Surveillance Service (PTSS)

The OA-IA worked intensively with the PTSS for Audit '21-16 Telecommunication services'. A meeting was held at the PTSS and the PTSS answered several of the OA-IA's questions. In addition, OA-IA auditors also underwent training at the PTSS on 22 November 2022 to learn more about the monitoring possibilities of the FIS.

Control Delegation (CDeI)

The CDeI invited the OA-IA to three hearings. The following topics were discussed:

- 26 January 2022: Reports for Audit '21-1 Deployment of FIS employees in Swiss representations abroad', Audit '21-2 Critical infrastructure protection/cyber defence' and reports on incidents in the Cyber FIS Division.
- 29 June 2022: Audit report for '21-15 HUMINT'; audit reports for subsequent Audit '22-18 Data collection by Cyber FIS' and Audit '22-16 Links between FIS and EOC and Swiss telecommunication service providers'.
- 22 November 2022: OA-IA prepares draft audit plan for 2023; OA-IA provides a legal assessment of an information-gathering measure requiring approval (IGMRA); interim results of Audit '22-18 Data collection by Cyber FIS'.

Independent Control Authority for Radio and Cable Communications Intelligence (ICA)

As part of the planned transfer of the ICA's tasks to the OA-IA as set out in the IntelSA, an OA-IA representative took part in the ICA's regular inspections of the intelligence services. The aim was to become familiar with the ICA's inspection methods

“The OA-IA can share oversight methods, processes and experiences with other oversight authorities working in the same field.”

and to ensure the transfer of know-how. In addition, the new Director of the OA-IA met with the president of the ICA on 25 October 2022.

Visit to the OA-IA by the head of the DDPS General Secretariat

On 15 March 2022, the head of the General Secretariat of the DDPS paid a courtesy visit to the OA-IA and took the opportunity to provide an update on recruitment of the new Director of the OA-IA.

Citizens

In 2022, the OA-IA received twenty-one enquiries from citizens.

Other meetings

In 2022, the Director of the OA-IA met at least once with the following people to discuss various matters:

- Head of DDPS
- Head of DDPS General Secretariat
- Director and deputy director of FIS
- Head of MIS
- Head of EOC
- Former head of SFAO
- Head of DDPS Internal Revision

7.2 International contacts

The OA-IA can share oversight methods, processes and experiences with other oversight authorities working in the same field. This brings continuous benefits to audit activities. How-

ever, the OA-IA (unlike intelligence services) has no legal basis for substantive information sharing with foreign partner authorities. The following international meetings took place in 2022:

Meeting with the Danish oversight authority (Tilsynet med Efterretningstjenesterne, TET), Bern

On 9 March 2022, the OA-IA met with the Danish oversight authority at the latter's request to exchange views on possible approaches to oversight. This included mapping of IT infrastructure, oversight communication strategies and how best to handle topics that receive considerable media attention. The OA-IA was able to learn from the Danish oversight authority about additional ways of mapping IT infrastructure. At the same time, the Danish oversight authority was inspired by the OA-IA's website and this prompted it to produce an explanatory video in 2022 similar to the one used by the OA-IA.

Intelligence Oversight Working Group (IOWG)

The IOWG is an international working group comprised of representatives of the oversight authorities of Belgium, Denmark, the Netherlands, Norway, England, Sweden and Switzerland.

- Bern, 10–11 March 2022 (IOWG Staff Level): The OA-IA organised this first face-to-face meeting since the pandemic. Topics included the structure of the working group, future areas of focus and various methods to be used to inform the public.
- London, 5–6 October 2022 (IOWG Staff and Chair Level): At the staff-level meeting, the oversight authorities exchanged views on oversight challenges associated

¹⁴ Art. 78 para. 2 IntelSA

with the (new) technological methods and means used by intelligence services. At the staff-level meeting, participants decided that additional member countries would be able to attend meetings. They also confirmed the jointly agreed statement.

Third Workshop of ‘European Intelligence Oversight Network (EION)’, 10 June 2022, Berlin

On 10 June 2022, two OA-IA staff members attended a workshop organised by the Stiftung Neue Verantwortung in Berlin.

The workshop focused on the collection and processing of commercially available data by intelligence services. In a technical presentation, the Dutch oversight authority (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD) explained the findings from their audit on the use of automated OSINT by the Dutch intelligence services. Automated OSINT is the automated collection of data from information sources that can be accessed by anyone using specialised software or web applications (tools). These tools include software that comes with search and network analysis features and offers a user-friendly way of retrieving information from a variety of different sources.

In two discussion panels, the participants also exchanged views on the legal basis and the tasks of oversight authorities with regard to the acquisition and use of commercially available data by intelligence services. By taking part in this workshop, the OA-IA gained in-depth background knowledge, which could ultimately be included in the planned Audit ‘22-15 Open-source intelligence (OSINT)’.

European Intelligence Oversight Conference (EIOC)

On 6–7 October 2022, the British oversight authority hosted an international meeting to discuss new technological challenges – such as artificial intelligence. All oversight authorities are currently working to introduce national legal bases to enable the exchange of information. Oversight authorities from the United Kingdom, Austria, Belgium, Bulgaria, Denmark, Finland, France, Germany, Greece, Italy, Luxembourg, Norway, the Netherlands, Portugal and Switzerland attended this meeting.

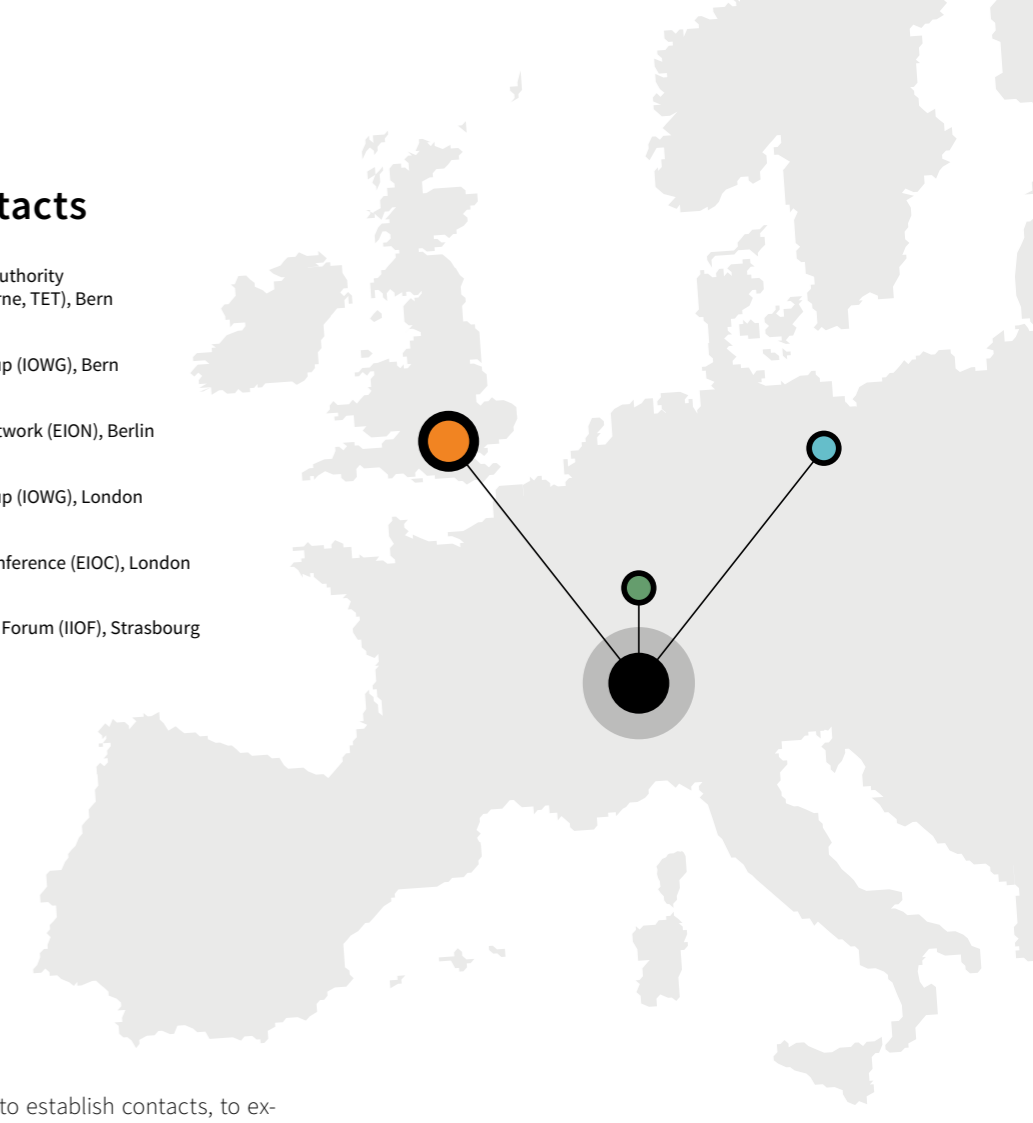
International Intelligence Oversight Forum (IIOF), 14–15 November 2022, Strasbourg

The fifth IIOF meeting took place in Strasbourg on 14 and 15 November 2022. In addition to OA-IA staff, participants at the event included members of intelligence oversight authorities, intelligence services and data protection authorities. Among the various topics, participants discussed implementation of Convention 108+, which sets minimum legal standards on the contracting parties with regard to data processing and protection of the rights of the persons concerned. Intelligence oversight is also affected by this. This is because the rules of Convention 108+ include exceptions when it comes to intelligence. The less stringent requirements placed on intelligence services must be balanced by stronger oversight. Other topics related to the current security situation and the development of intelligence techniques and technologies.

With the digital transformation of society, the challenges created by cyberspace and the emergence of new tools to search for and process information, such interactions with other oversight authorities is invaluable for the OA-IA. In particular,

International contacts

- Meeting with the Danish oversight authority (Tilsynet med Efterretningstjenesterne, TET), Bern 9 March 2022
- Intelligence Oversight Working Group (IOWG), Bern 10–11 March 2022
- European Intelligence Oversight Network (EION), Berlin 10 June 2022
- Intelligence Oversight Working Group (IOWG), London 5–6 October 2022
- European Intelligence Oversight Conference (EIOC), London 6–7 October 2022
- International Intelligence Oversight Forum (IIOF), Strasbourg 14–15 November 2022



such meetings make it possible to establish contacts, to examine oversight practices, to find out about the experiences of other oversight authorities, and to share and develop best practices in the area of oversight.

Meeting with Canadian oversight authority (National Security and Intelligence Review Agency, NSIRA), 17 November 2022, Bern

On 17 November 2022, the OA-IA welcomed a delegation from the Canadian National Security and Intelligence Review Agency (NSIRA). This meeting in Switzerland took place at NSIRA's initiative after NSIRA representatives had attended the IIOF in Strasbourg on 14 and 15 November.

The discussions focused in particular on the structure, legal framework and procedures of the Swiss and Canadian oversight authorities. After touching on theoretical aspects, the participants exchanged views on the respective best practices in intelligence oversight. The OA-IA staff also shared their experiences with public relations, and the NSIRA representatives were positively impressed. All of the participants concluded that the meeting had been productive.

8. Appendix

8.1 Audit Plan for 2022

No.	Name of audit	Service audited
Strategy and Planning		
22-1	Anticipation and early detection	FIS ¹
Organisation		
22-2	Business Continuity Management and Disaster Recoveries in IT operations	EOC ²
Cooperation		
22-3	Audit of CIS Valais	CIS ³ / FIS
22-4	Audit of CIS Glarus	CIS / FIS
22-5	Audit of CIS Thurgau	CIS / FIS
22-6	Audit of CIS Zug	CIS / FIS
22-7	Audit of CIS Schwyz	CIS / FIS
Information gathering		
22-8	Operations, operational clarifications and information gathering measure requiring authorization	FIS
22-9	Human Intelligence (HUMINT ⁴)	FIS
22-10	Information gathering by measures not requiring authorization	FIS
22-11	Information gathering management	FIS
22-12	Sensor control and selection in military intelligence	MIS ⁵
Resources		
22-13	Clandestine cash flow	FIS
22-14	Recruiting-, support- and leaving process	FIS
Data Processing / Data Storage		
22-15	Open Source Intelligence (OSINT ⁶)	FIS

¹ Federal Intelligence Service

² Electronic Operations Center

³ Cantonal Intelligence Service

⁴ Human Intelligence, gathering information from human sources

⁵ Military Intelligence Service

⁶ Open Source Intelligence, gathering information from public sources



8.2 Abbreviations

Art. Article	IOWG Intelligence Oversight Working Group
BBL Federal Gazette	MIS Military Intelligence Service
BCM Business Continuity Management	N-SIS National section of Schengen Information System
CDeI Control Delegation of the Swiss Parliament	OA-IA Independent Oversight Authority for Intelligence Activities
CIS Cantonal intelligence services	OSINT Open-source intelligence, intelligence information derived from publicly available sources
DDPS Federal Department of Defence, Civil Protection and Sport	Para. Paragraph
EOC Electronic Operations Centre	pp. Subsequent pages
FAC Federal Administrative Court	PSS Personnel security screening
fedpol Federal Office of Police	PTSS Post and Telecommunications Surveillance Service
FIS Federal Intelligence Service	RIPOL Computerised police search system
HUMINT Human Intelligence, gathering information through human sources	rsp. respectively
i.a. Inter alia	SFAO Swiss Federal Audit Office
ICA Independent Control Authority for Radio and Cable Communications Intelligence	SR Classified Compilation of Federal Legislation
IM Information Management	
IntelSA Federal Act of 25 September 2015 on the Intelligence Service (Intelligence Service Act; SR 121)	
IntelSO Ordinance of 16 August 2017 on the Intelligence Service (Intelligence Service Ordinance; SR 121.1).	



Historical school building in Schwyz

**Independent Oversight Authority
for Intelligence Activities**

Maulbeerstrasse 9, 3003 Bern

Phone +41 58 464 20 75

www.ab-nd.admin.ch