Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Independent Oversight Authority for Intelligence Activities

Annual Report 2020
of the Independent Oversight Authority for Intelligence Activities OA-IA

1. Summary

The Independent Oversight Authority for Intelligence Activities (OA-IA) was able to carry out sufficient audit activities to implement its oversight mandate despite corona-related restrictions. Deep insights were gained from the audits of five cantonal intelligence services (CIS), from review of the information system used by the Federal Intelligence Service (FIS) and from the FIS' handling of information requests. Operational activities were examined from various angles. With an unannounced audit at the FIS, the OA-IA gained clarity regarding the locations and summary contents of FIS archive rooms. With increasing experience and a consistent team composition, OA-IA audits are also becoming more complex and in-depth, because interrelationships and dependencies are now better understood.

Looking back on the past year, the OA-IA considers that there are three areas where there is need for improvement at the FIS. Reporting to the Federal Council was the subject of several audits concerning partner services, operational investigations or information gathering through human sources (human intelligence, HUMINT). Here the question that needs to be settled is what and how much information should be provided to the head of the Federal Department of Defence, Civil Protection and Sport (DDPS) in order to be able to take political responsibility and how much discretion should the FIS enjoy in deciding what and how much to report in order to act with sufficient agility.

In the area of information technology, the OA-IA noted that the complexity of user rights management for systems and applications continues to challenge the FIS. Finally, the OA-IA considered the FIS' unequal handling of information requests to be problematic. The preferential handling (i.e. prioritisation and more detailed responses) of information requests from politicians and journalists compared to the handling of information requests from ordinary citizens violates the requirement of equal treatment under Article 8 of the Federal Constitution[1].

The discussions with the FIS were constructive, whereby the service can be said to have a certain capacity for self-criticism. In many areas, OA-IA recommendations trigger action whose necessity had already been recognised internally, at least in part.

The Military Intelligence Service (MIS) was audited by OA-IA to assess its information sharing arrangements with foreign partners and its information system landscape. The latter was an exploratory audit. Among other things, the OA-IA recommended that the MIS should consider standardising its products and data in order to facilitate cross-platform data exchange within the Swiss Armed Forces and with its partners. For the Electronic Operations Centre (EOC) – and similarly for the FIS – risks were identified in the area of supplier management. However, there is little room for manoeuvre due to the reduced number of suppliers available. Nevertheless, the risks of information leaks can be minimised through more in-depth independent background checks of the suppliers' environment to the extent permissible by law.

The 2020 Annual Report was prepared in consultation with the DDPS and the Control Delegation of both the National Council and the Council of States from 12 January to 10 February 2021. Where feedback indicated formal or material errors in the Annual Report or interests worthy of protection that precluded publication of certain parts, these were taken into account.

[1] SR 101

Conclusion

The OA-IA formulated 55 recommendations in relation to the 17 audits conducted. Implementation of these recommendations will enable existing risks of intelligence activities can be further reduced and result in efficiency gains.

The desire to fulfil its mandate as best as possible within the legally prescribed framework is palpable at the FIS. It has managed to achieve this to a greater extent in operational dealings with its partners. However, it has had more difficulty making the necessary operational adjustments and optimising the complex environment of data storage in its information and archive systems. The OA-IA feels that further efforts are needed in these areas. The FIS is willing to face the challenges and to take new directions where necessary.

Less clearly defined, but also less risky, was the alignment of the MIS. With an adapted basic mandate recommended by the OA-IA, there is now a basis for further work to be done. At EOC, technological advances and newly available possibilities are most noticeable. It therefore makes sense for the OA-IA to take stock of the current situation and consciously reflect on the path taken thus far and the way forward.

2. Table of Contents

3. Personal

"Oversight is not a universal solution to a lack of trust, but it can strengthen trust in the intelligence service."

Thomas Fritschi

Thomas Fritschi, OA-IA Director

Oversight and control have become buzz words in national policymaking circles. We are all familiar with the saying 'Trust, but verify'. So is control the solution to a lack of trust in the intelligence service? The FIS is aware of OA-IA oversight activities. Our audit activities are accepted, perceived as serious and competent. Errors can indeed be found and corrected through inspections, such as violated regulations on the deletion of data or incomplete documentation of guidance of human sources.

Whether data theft or cases similar to that of Crypto AG can be completely prevented by conducting control and oversight activities is unlikely as such incidents are the result of deliberate action. Defensive precautions, rules on who does what and data storage can all be verified, but the will and ideas of people (fortunately) cannot. This also applies to intelligence service personnel. In order to achieve maximum security against abuses, trust is ultimately needed. This trust is strengthened by continuous controls that lead to a constructive outcome. If mistakes are discussed and corrected in a supportive manner, then this can also serve as a confidence-building measure. Oversight is not a universal solution to a lack of trust, but it can strengthen trust in the intelligence service.

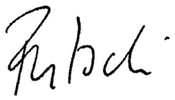
As an oversight authority, we act on behalf of the population, so to speak. We also rely on the trust of the population in our work. We have to earn this trust through truthful, transparent, timely and clear communication. Among other things, this Annual Report serves this purpose.

The pandemic has also affected OA-IA activities. We therefore cannot avoid reporting on this in the 2020 Annual Report. However, intelligence services and the OA-IA had to adapt to the new situation. Sick staff, working from home and a massive reduction in direct human contact have changed the usual procedures and possibilities. However, OA-IA managed to adhere to the established audit plan for the most part. A small number of interviews did not take place on site but were conducted via email. Despite all this, we were able to gain in-depth insights into the intelligence activities during the reporting year.

Only in passing will we report here on the case of Crypto AG. The OA-IA was informed of the incident by the head of the DDPS on 12 November 2019. In February 2020, the Control Delegation (CDel) decided to conduct an investigation into the matter. The corresponding report was presented to the public on 10 November 2020. In response to these developments, the OA-IA decided, in consultation with the CDel, to conduct an unannounced audit and inspected FIS file depots.

Our Annual Report is intended to present the results of our auditing activities and provide interested readers with background information and context on intelligence activities. For this year's report, we have chosen the topic of control and oversight. You will learn why and how we conduct our audits. Furthermore, André Duvillard, the Federal Council's delegate to the Swiss Security Network, shares his view from outside as a proven expert on intelligence oversight issues.

I hope you enjoy reading this report.



Thomas Fritschi, OA-IA Director

4. Control and oversight

Performing audit procedures and control activities is part of the OA-IA's core remit. In this Annual Report, we therefore cover selected aspects of our main activity. This chapter highlights our audit methods, introduces the various types of audits and explains who oversees OA-IA activities.

4.1 OA-IA audit methods – How does the OA-IA audit legality, effectiveness and expediency?

The OA-IA has access to all relevant information and documents as well as access to all premises of audited intelligence services. It also has the possibility of requesting copies of documents. In its oversight activities, it may also request further information and authorisation to inspect files of other federal and cantonal agencies, insofar as this information relates to cooperation between these agencies and the audited services.

In order to carry out its oversight activities, the OA-IA may request access to the information systems and data collections of audited intelligence services as required for the audit and may also access sensitive personal data. This is a basic requirement in order to be able to examine the legality, effectiveness and expediency of the intelligence activities at all.

Reasonable care must be exercised when conducting an audit. The auditor's judgement and knowledge of the audit subject are fundamental prerequisites for conducting an audit. Reasonable care includes, among other things, complete and comprehensible preparation and documentation of the audit procedures. When ascertaining and assessing facts, it is essential to record any deviations from requirements in an open, clear and justified manner. Given the highly diverse professional background and different levels of initial and continuing training of OA-IA staff, it is essential that the various requirements and audit methods are clearly regulated. This is the only way to ensure the most uniform approach possible. OA-IA has established internal procedures for this purpose.

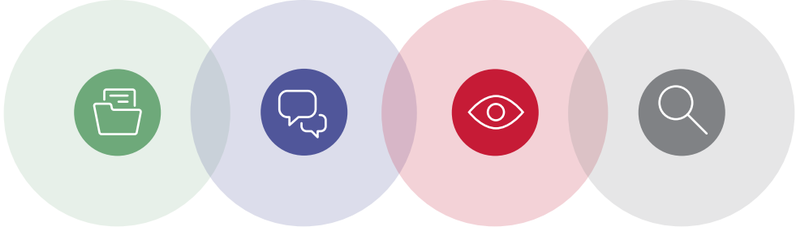
The OA-IA uses, among others, the following audit methods to obtain audit evidence:

- Inspection
- Observation
- Interviews
- Random sampling

Inspection

Inspection consists primarily of checking records and documents. It provides audit evidence with varying degrees of reliability, depending on whether the documents were provided by the audited party or by third parties or whether the OA-IA was able to independently gain access to these documents in the various systems. Inspection can only be carried out on existing and accessible documents; information that is not documented by the services cannot be audited by OA-IA.

Audit methods



Observation

Observation consists of examining a process or procedure. To do this, OA-IA bases its judgement on live demonstrations of a particular operation by staff from the audited services. This has the added advantage that OA-IA can come into direct contact with staff at all levels who are otherwise less likely to be affected by audits.

Interviews

Interviewing consists of obtaining information from persons inside or outside the entity to be audited. Interviews range from formal written enquiries with third parties to oral interviews with persons of the body to be audited. In the case of oral interviews, the interviewees are informed in advance of their obligation to answer the questions asked truthfully and completely. The persons interviewed must not suffer any disadvantage from their statements. This certainty and legal support is elementary in order to give the interview partners sufficient security to also address sensitive and unpleasant topics. Answers in interviews can provide auditors with important new information or corroborate previous audit evidence.

"The auditor's judgement and knowledge of the audit subject are fundamental prerequisites for conducting an audit."

“Random sampling is a suitable auditing method, especially when analysing and assessing large volumes of data.”

Random sampling

Random sampling is a suitable auditing method, especially when analysing and assessing large volumes of data. The aim is to be able to make as reliable a statement as possible about the total amount of data using a sufficiently large number of samples. The selection of samples is decisive in this case.

When considering the desired outcome of their audit, auditors also make sure that the workload placed on both auditors and audited bodies remains proportionate. In particular, interviews, meetings and the burden of parallel audits must be included in this consideration. Before any contact is made, the OA-IA checks in advance whether documents, regulations, directives, etc. are not already available to it or can be retrieved independently from the information systems of the audited services.

Audit durations may extend over several months. The information obtained through the aforementioned audit methods is used by the OA-IA to prepare an audit report, which is then submitted to the audited body for comment. The audited body’s feedback is then included in the audit report and the report is sent to the head of the DDPS. Any discrepancies are resolved in advance, if possible, or identified as such in the report.

4.2 Coordinated, announced and unannounced audits

Coordinated audits

In 2020, the OA-IA coordinated its own audits of CIS with the audit conducted by the Swiss Federal Audit Office (SFAO). The SFAO is preparing its own report entitled ‘Subsidies to cantonal intelligence services’. Audit preparations and to a lesser extent implementation aspects were discussed and coordinated by SFAO and OA-IA audit managers. Both oversight authorities were free to draw their own conclusions. This approach improves the effectiveness of audits and reduces the burden on the audited bodies. Apart from this, methods can be exchanged and optimised. This procedure is not suitable for every audit topic, but can make sense for individual cases.

Normal situation – announced audits

Each year, the OA-IA creates an audit topic repository in which the auditors enter possible audit topics or ideas. In the third quarter of each year, the OA-IA holds a retreat to develop the audit plan for the following year. A risk analysis of the audit proposals contained in the audit topic repository is carried out and a provisional audit plan is drawn up. The OA-IA Director consolidates the audit plan and submits it for consultation to the head of the DDPS, to the audited bodies (FIS, MIS and EOC) as well as to the other intelligence service oversight bodies. At the end of the year, the audit plan for the next year is finalised and published on the OA-IA website. The audits are thus announced.

Exceptional cases – unannounced audits

The OA-IA reserves the right to conduct unannounced audits. It hopes that unannounced audits will provide more immediate and direct insight into the circumstances of the audited bodies.

The Federal Act on the Intelligence Service (IntelSA)[2] authorises the OA-IA to gain the necessary access to relevant information. The OA-IA also has access to all premises of the audited agencies and can also access all their information systems and data collections. In practice, information protection measures may in some circumstances make unannounced entry to buildings or access to information difficult. This fact must be taken into account through meticulous planning. Such an audit also places a greater burden on the audited body: Responsible personnel must be called up ad hoc during ongoing operations and access must be organised. Further-

[2] SR 121

“The OA-IA performs its function independently and is not bound by instructions.”

more, the OA-IA must be provided with premises in which it can carry out its audit activities and hold meetings without interruption.

The developments surrounding the Crypto AG case prompted the OA-IA to offer its assistance to the CDel in examining existing FIS archives. The OA-IA subsequently audited FIS archives without prior notice. Information about ‘Audit 20-19 Archives’ can be found in Section 5.2.

4.3 Who oversees OA-IA activities?

‘Who watches the watchmen?’ was the headline of the ‘Tages-Anzeiger’ in mid-2017. ‘Who oversees the OA-IA?’ is still a legitimate question today. The OA-IA performs its function independently and is not bound by instructions. This is an important change brought about by the IntelSA, which gives the OA-IA free reign in selecting and deciding audit topics. Administratively, it is assigned to the DDPS. The administrative assignment to a federal department reduces infrastructure and logistics costs, which would otherwise be much higher. Technical synergies within the Federal Administration in particular can be used well in this manner. However, OA-IA independence does not mean that is free of oversight. Quite the opposite: the OA-IA is subject to oversight by a large number of bodies.

The OA-IA has its own accounts and budget. Both must be presented and proposed to the Finance Committees of the National Council and the Council of States on an annual basis. In addition, the SFAO has the power to audit the OA-IA (as a decentralised federal agency) to verify compliance, legality and cost-effectiveness. Finally, the CDel exercises parliamentary oversight of the OA-IA. It thus has access to all OA-IA documents and information and can summon OA-IA staff to hearings.

However, the OA-IA is not only subject to oversight by the Federal Administration or Parliament. The public also plays an important role. The media, individual politicians and citizens respond to OA-IA publications. Their published statements are noticed and commented on. These reactions are also an indicator of the expectations placed on the OA-IA. We take comments from the public into account and follow up on them. While we are unable to satisfy all requests to the same extent, they are all valuable for our audit work.

Finally, there is also oversight from the audited agencies themselves, which receive all audit reports for comment before these reports are sent to the head of the DDPS. Obvious errors and misunderstandings can thus be clarified and corrected, and any differences can be commented on.
We value all these checks and use the feedback we receive to continuously improve our performance so that trust in us as an oversight body is further strengthened.

Who oversees OA-IA activities?

“The OA-IA is subject to oversight by a large number of bodies.”

Audited agencies by the OA-IA

5. Oversight activities

"For the first time, the OA-IA also conducted an unannounced audit in 2020."

For this Annual Report, OA-IA has changed its reporting policy on the audits performed. We have set priorities and will now provide detailed information only on selected audits in 2020 and no information at all on other audits. However, the summarised findings of each audit are available on the OA-IA website.[3]

5.1 Audit plan

The OA-IA prepares an audit plan each year.[4]

The audit topics for 2018 and 2019 were grouped into seven audit areas. For the 2020 audit period, the OA-IA decided to merge the two audit areas 'Operations' and 'Information-gathering measures requiring approval (IGMRAs)' into a single audit area 'Information gathering':

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

5.2 Audits conducted in 2020

A total of 18 audits were planned for 2020. For the first time, the OA-IA also conducted an unannounced audit in 2020.

Due to corona-related restrictions, audit activities had to be reduced between March and May, as well as in autumn 2020. This delayed the performance of individual audits.

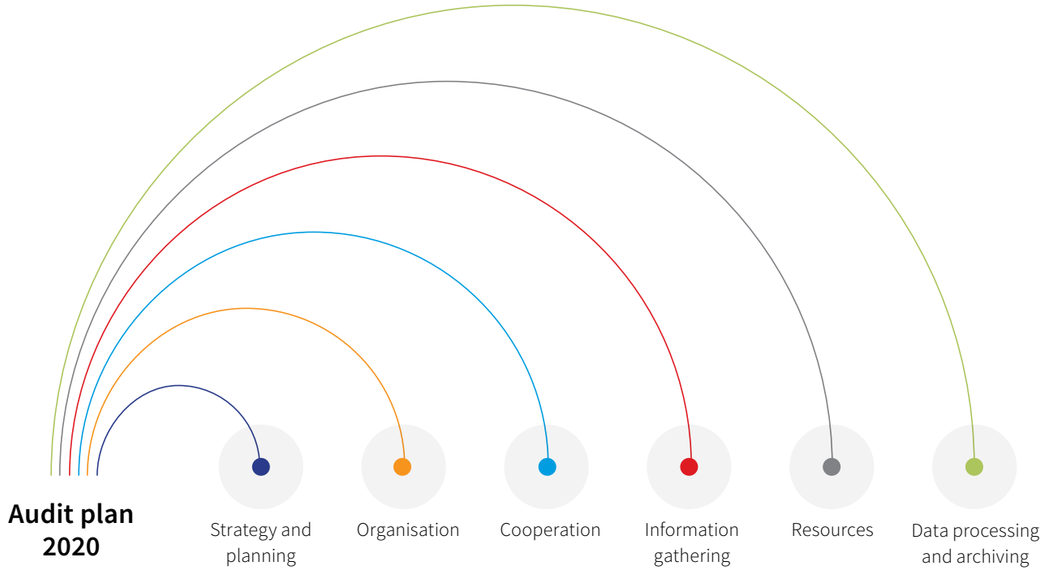
Over the course of 2020, one audit from 2019 was completed. Of the planned 18 audits, 13 audits were completed by the end of the year with a report sent to the head of the DDPS. For three audits, the audit procedures were completed by the end of 2020 and the reports were submitted to the head of the DDPS in the first quarter of 2021. One audit was postponed until 2021 due to restructuring of the audited services and another audit was not carried out at all in the planned form. In addition, one unannounced audit took place.

The OA-IA relied more on written and telephone interviews due to corona-related restrictions and where possible adhering to information protection regulations. Such interviews from a distance cannot always replace personal interview in terms of quality. However, given the circumstances, this approach enabled the OA-IA's oversight activity to continue.

Audit '20-1 Change Management' is the only audit that was not able to be started in 2020 and will therefore be addressed at a later date in an adapted form. Audit '20-3 Allocation of FIS and MIS roles and responsibilities in the area of analysis' was only started in December 2020, which is why we cannot provide information about this audit in the present report.

In the reporting year, the OA-IA conduct short-term individual inquiries in three cases, based on current events or developments (e.g. the Crypto AG case), with a view to a possible audit. Some of the insights gained from these inquiries were included in ongoing or planned audits.

[3] www.ab-nd.admin.ch
[4] See Section 4.2 'Coordinated, announced and unannounced audits'.



5.2.1 Strategy and planning

In the area of 'Strategy and planning', audits focus on topics relating to short-, medium- and long-term strategic planning of the intelligence services in Switzerland as well as their objectives. The following audits were planned in 2020:

- 20-1 Change management (FIS, MIS, EOC audit not carried out)
- **20-2 Additional resource requirements (FIS)**

20-2 Additional resource requirements (FIS)

One hundred days after taking office, FIS Director Jean-Philippe Gaudin carried out an initial assessment of the situation on 19 October 2018. He explained at the time that entry into force of IntelSA had generated additional legal and administrative work. To ensure that this additional burden did not impair the FIS' actual core intelligence activities, the then head of the DDPS allocated additional resources to the FIS by creating 28 new posts. At that time, the FIS Director stressed that these 28 new posts would not be sufficient. And even prior to that, the FIS had been granted 16 new posts in 2017 with the then new IntelSA and a further 23 posts in 2015 for the Counterterrorism.[5]

On 3 July 2019, the Federal Council followed up on a request by the DDPS to create an additional 100 posts at the FIS. In 2019 and 2020, the DDPS allocated 40 of these 100 posts to the FIS through intra-departmental transfers. The remaining 60 posts will be added in 2021, 2022 and 2023 in equal parts of 20 posts each year, subject to parliamentary approval in each case. The posts would primarily be used for counter-terrorism and countering violent extremism. In addition, CIS staff numbers within cantonal police corps will be increased. The Federal Council has allocated an annual budget of CHF 2.6 million for this purpose, thus creating 26 new posts. With an additional CHF 3 million per year, existing surveillance units in the three cantons of Bern, Vaud and Zurich were expanded to facilitate their work with the FIS.

[5] DDPS press release 'Federal Council creates additional counter-terrorism posts', dated 18 December 2015, www.vbs.admin.ch/de/aktuell/medienmitteilungen.detail.nsb.html/60085.html

At the end of 2019, the Federal Assembly adopted in a federal decree that the remaining 60 posts to be created for the FIS according to the 2021 - 2023 financial plan would be paid out of the DDPS current personnel budget - i.e. contrary to Federal Council's proposal of creating the positions by raising the maximum cap on new posts.[6] As a result, the DDPS proposed in autumn 2020 that the corresponding funds needed for the required personnel and workplace expenditures would be drawn from the DDPS' budget allocation for armament and capital expenditure so that the posts could be created in a budget-neutral manner. This proposal was also accepted by the Finance Committee's subcommittees. The FIS will thus receive 60 new posts over the next three years, subject to parliamentary approval.

The FIS can easily absorb an annual increase of 20 posts each (including staff turnover) and handle this through normal HR management processes. In its Audit '20-2 Additional resource requirements', the OA-IA found that FIS does not require job marketing as it has no difficulty filling its job vacancies. In order for the FIS to face the planned increase in staff in an expedient and effective manner, it relies on various strategic HR management activities. In this way, the FIS has adopted a serious, longer-term planned and managed approach to the upcoming increase in posts.

Recruitment for the 40 additional DDPS-funded posts has largely been completed. The FIS is an interesting and appealing employer, which is clearly underscored by the number and quality of the applications received and by the calibre of newly hired staff. In addition to the extra effort needed to recruit, induct and train new recruits, the increasingly limited space constitutes a serious challenge for the FIS. The new construction project pursued by the Federal Office for Buildings and Logistics (FOBL) to replace the current buildings will be completed in several stages over a period of about ten years.[7]

Once recruitment has been completed at the end of 2023, the OA-IA will conduct an audit to determine whether the posts have been filled in accordance with the priorities set by the Federal Council Security Committee (FCSC). After that, an audit will be conducted to assess the extent to which the compensation paid to the cantons for their surveillance activities has proven adequate and whether the distribution of additional compensation to the CIS has been handled on the basis of clear and binding criteria.

5.2.2 Organisation

In the area of 'Organisation', the OA-IA examines whether the structure of the services and their processes enable them to fulfil their legal mandate as lawfully, expediently and effectively as possible.

In 2020, the OA-IA started the audit mentioned below. At the time this report was sent for publication, the work had not yet progressed to the point where the results could be included in the report.

- 20-3 Allocation of powers and responsibilities between FISA-MIS

[6] Art. 2 let. o in Federal Decree II on the Financial Plan for the period 2021-2023, dated 12 December 2019

[7] FBL media release 'Project competition for new DDPS administration centre has been decided', 16 July 2020, www.bbl.admin.ch/bbl/de/home/dokumentation/nsb-news-traegerseite.msg-id-79864.html

"Cooperation between the FIS and the CIS improves."

5.2.3 Cooperation

This audit area covers national and international cooperation between intelligence services. The CIS are an annual focal point of the OA-IA's audit activities.

In 2020, OA-IA conducted the following audits:

- **Audit 20-4 CIS St. Gallen (FIS)**
- **Audit 20-5 CIS Zurich (FIS)**
- **Audit 20-6 CIS Ticino (FIS)**
- **Audit 20-7 CIS Solothurn (FIS)**
- **Audit 20-8 CIS Fribourg (FIS)**
- Audit 20-9 Partner services (FIS and MIS)
- Audit 20-10 Cooperation with partners at federal level (FIS)

Audits of CIS in 2020

In 2020, the OA-IA reviewed the intelligence activities of the CIS of the Cantons of St. Gallen, Zurich, Ticino, Solothurn and Fribourg as well as their cooperation activities with the FIS. The OA-IA has thus audited a total of 10 CIS[8] since its inception. The OA-IA will audit the remaining 16 CISs over the next three years.

The conclusion drawn in all of the CIS audits conducted in 2020 was that cooperation between the FIS and the CIS can be described as 'better than before'. This was due in part to the greater efforts made at the FIS to work with CIS and to the increased allocation of resources to the cantons.

The increase in the number of posts in the CIS combined with the greater transfer of resources to place using a distribution key determined by the FIS Director and agreed with the Conference of Cantonal Police Commanders of Switzerland (CCPCS).The cantons that were allocated additional posts[9] were able to complete most of the expansion work by the end of 2020. The posts were allocated selectively to support individual FIS areas of activity and have already begun to have an effect. The CIS that were granted resources can now better manage their mandates and address issues that were previously not dealt with due to capacity constraints.

20-4 CIS St. Gallen

CIS St. Gallen completed its FIS assignments on time, provided the requested information and demonstrated good intelligence expertise. The number of spontaneous reports to the FIS provided for the years 2017 to 2019 was, in the view of the OA-IA, rather low for a CIS equipped with six full-time posts. CIS St. Gallen maintains three lists of personal data broken down by subject. These lists include a total of 135 registered persons. In principle, CIS St. Gallen is allowed to keep such lists of personal data in the CIS filing system. However, since the FIS has a tool at its disposal in the form of the CIS specialist application (SA CIS), which includes a structured filing feature, the OA-IA did not consider it expedient to keep such lists. The OA-IA formulated a corresponding recommendation. It was also suggested that the FIS and CIS St. Gallen consider whether the current allocation of one full-time position to each of the five regions (i.e. five employees) is optimal.

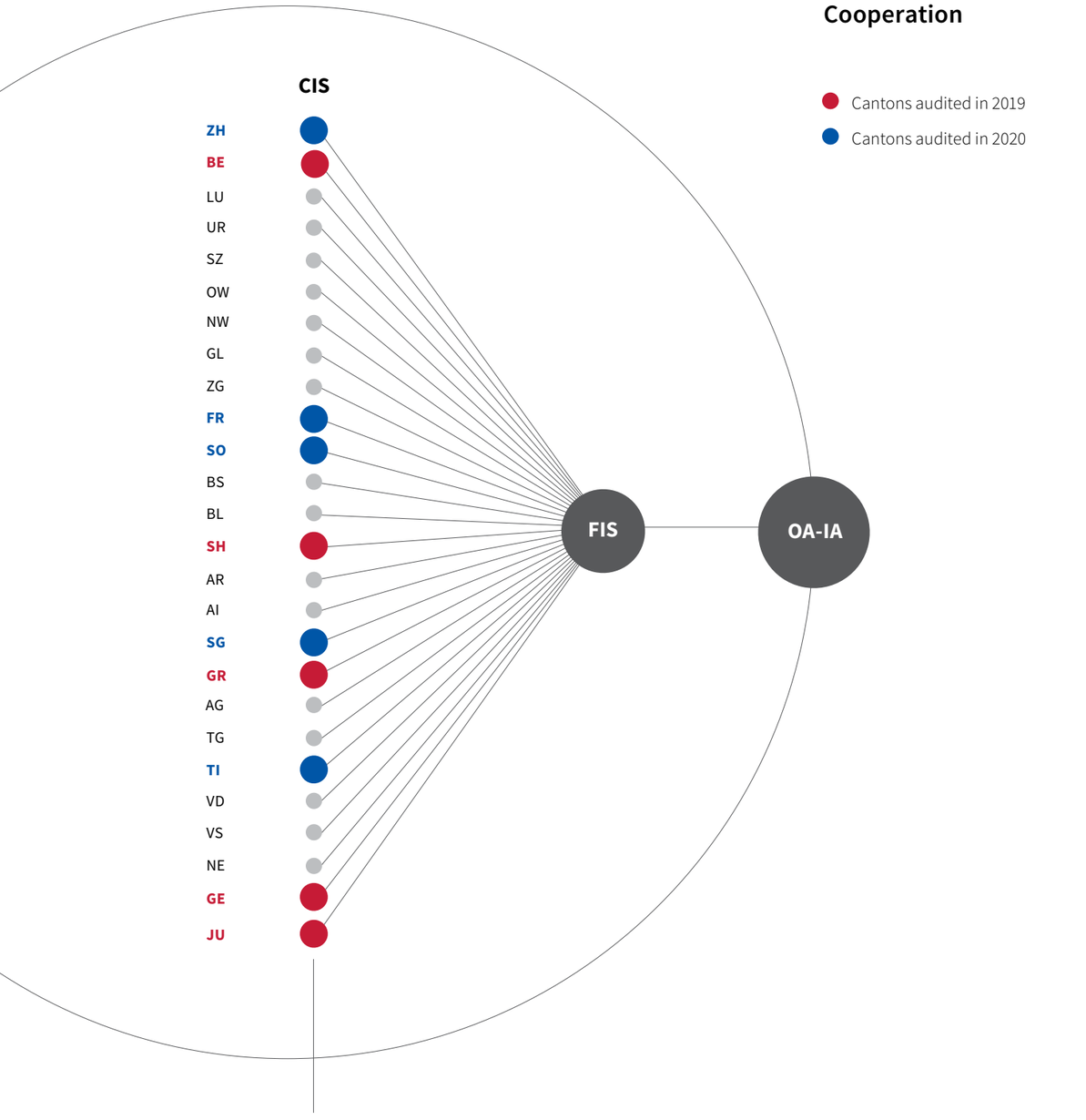
20-5 CIS Zurich

With CIS Zurich, the OA-IA audited one of the largest CIS in Switzerland. It audited a sample from a total of 30 assignments awarded to CIS Zurich by the FIS. Among other things, the audits examined the purpose of information gathering, the actions taken, the results achieved and compliance with the deadlines set. Based on the results of this sample, on its

[8] In 2019, the OA-IA reviewed the CIS of Bern, Graubünden, Geneva, Jura and Schaffhausen.

[9] One job position corresponds to CHF 100,000 in compensation.

Cooperation



Cantons audited in 2019

Cantons audited in 2020

150 FTEs

own observations and the feedback that the FIS gave in its performance assessment, the OA-IA concluded that CIS Zurich follows the orders given to it in a timely and satisfactory manner.

The FIS and CIS Zurich work closely together and very well in most areas. In one thematic area, however, things are not running optimally at the FIS from the perspective of CIS Zurich. Different viewpoints on organisational aspects, the design of missions and the corresponding use of limited resources are justifiable and understandable. However, the OA-IA feels that it is important that the FIS and CIS Zurich discuss these different viewpoints and that any differences be resolved.

The OA-IA was able to find files on both the CIS filing system and the SA CIS that were not deleted as they should have been during the data migration from the cantonal information system to that of the FIS in 2017/2018. The OA-IA formulated a corresponding recommendation here as well.

The Zurich Cantonal Police's observation group set up to work with the FIS is already being used today and will also be deployed outside the Canton of Zurich in the future with the new performance mandate. The OA-IA is of the opinion that with CIS Zurich and in particular with the observation group, the FIS has efficient and reliable partners on its side. Furthermore, the OA-IA feels that very good conditions have been created with the integration of CIS Zurich into the overall structure of the Cantonal Police Zurich, with the unburdening of CIS from additional tasks and with the spatial separation of the CIS from the rest of the Cantonal Police (in particular from the Criminal Investigation Department). These measures ensure that CIS Zurich can focus on its tasks under IntelSA. The OA-IA therefore considers the compensation paid by the Confederation to have been used expediently.

20-6 CIS Ticino

CIS Ticino completed its FIS assignments on time and provided the requested information. Its services are of good quality and are appreciated by the FIS. The availability of an FIS liaison officer is an added value appreciated by CIS Ticino, despite the major workload resulting from the distance. In the usual exchange of information between the FIS and CIS Ticino, language does not seem to be a hinderance. However, details can be misunderstood in certain situations. It is therefore important that the FIS and CIS Ticino consult each other in case of ambiguities in order to clear up any doubts resulting from the language barrier.

20-7 CIS Solothurn

CIS Solothurn also has good intelligence expertise and is strongly committed. However, it has some catching up to do in the area of Prophylax approaches[10]. In addition CIS Solothurn doesn't always use the communication and data processing solutions provided by the FIS in an expedient manner. The OA-IA therefore recommended that the FIS, together with CIS Solothurn, review the use of these tools and, if necessary, provide additional training to the staff concerned. The OA-IA recommended that the FIS and CIS Solothurn review the existing allocation of intelligence work to the number of staff employed - as was also recommended to CIS St. Gallen.

20-8 CIS Freiburg

The OA-IA also reviews the CIS according to the criteria of legality, expediency and effectiveness. CIS Fribourg met all three criteria in the audit. It provides good quality intelligence services which are appreciated by the FIS. Some issues raised by the OA-IA have already been clarified and specified thanks to priority follow-up. These topics also included the list of the VIGIPOL staff used by the Fribourg Cantonal Police,[11] which was the subject of a recommendation.

As the OA-IA already noted in 2019, the CIS are the eyes and ears of the FIS on their own territory. They are an indispensable part of Switzerland's security network.

[10] FIS prevention and awareness programme
[11] After the attacks in Paris in January 2015, the Fribourg cantonal police created a unit called VIGIPOL.

"Those means of information gathering that can intrude most deeply into the privacy of the persons concerned receive special attention from the OA-IA."

5.2.4 Information gathering

Information gathering is a core task of intelligence services. They can use various means for this purpose. Those means that can intrude most deeply into the privacy of the persons concerned receive special attention from the oversight authority. These include IGMRAs, each of which is embedded in an intelligence operation. Due to this symbiosis, the two audit areas 'Operations' and 'Information-gathering measures requiring approval' were merged for the year 2020.

Likewise, information gathering through human sources is fraught with many risks. Therefore, management of human sources was again reviewed in 2020 for legality, expediency and effectiveness. This area is subject to confidentiality, which is why we do not discuss it further in this report.

The OA-IA conducted the following audits in this area in 2020:

20-11 Operations (incl. IGMRAs, FIS)
20-12 Human sources (FIS)
20-13 Operational clarification needs (FIS)

20-11 Operations (incl. IGMRAs, FIS)

Intelligence operations are a key element of information gathering for the FIS. Related processes can be managed as intelligence operations if they go beyond the extent, scope, workload or secrecy requirements of normal activities. Due to its importance, information gathering is included in at least one audit in the OA-IA audit plan each year.

In addition to auditing selected operations, the OA-IA conducted an audit of operational clarification needs for the first time last year. The FIS understands this term to mean more complex intelligence activities of lower intensity than that of operations. Unlike operations, for which there is an obligation to report to the head of the DDPS, there is no such obligation for operational clarification needs.

IGMRAs are another important element of intelligence gathering. Within the framework of an intelligence operation, both information-gathering measures not requiring approval (for example, observations in public and generally accessible places) and IGMRAs (for example, surveillance of post and telecommunications) can be used. However, if the FIS wishes to carry out IGMRAs, this may only be done as part of an intelligence operation. For this reason, the OA-IA decided to examine these two topics together in the reporting year – unlike what had been done in previous years.

The combined audit of operations and IGMRAs was launched in autumn 2020 and had not been completed at the time this Annual Report went to press. This audit comprised three parts: In the first part, a selected number of intelligence operations were reviewed for their legality, expediency and effectiveness. The second part examined whether the information-gathering measures approved by the Federal Administrative Court and the Federal Council had been implemented in accordance with these decisions. Finally, in the third part, auditors checked to see whether and to what extent the FIS had implemented the OA-IA's prior recommendations in the area of information gathering.

Without anticipating the final audit results, it could already be stated at the time of writing the annual report that the number of operations conducted was at a similar level as in the previous year. The audit procedures carried out so far have not revealed any irregularities worth mentioning. The FIS appears to have made comparatively less use of the IGMRAs instrument than in recent years. In addition to the current situation, the process of having to first obtain FAC and Federal Council approval as well as the time-consuming task of analysing collected data could be reasons for this. The FIS has completed several of the OA-IA's previous recommendations to the FIS in the area of information gathering, which clearly indicates a desire on the part of FIS officials to implement OA-IA recommendations. Moreover, the quality of implementation has now been confirmed in the audit.

"The FIS makes comparatively less use of the IGMRAs."

20-13 Operational clarification needs (FIS)

Audit '20-13 Operational clarification needs' was completed. Focusing on the topics of 'violent extremism' and 'non-proliferation', the OA-IA examined whether the selected operational investigations were conducted lawfully, expediently and effectively. In this audit, the OA-IA asked itself how operational clarifications could be distinguished from operations. In doing so, the OA-IA found that there were no formal criteria for opening operational clarifications. The OA-IA therefore made a recommendation to this effect. The purpose is to clarify which processes may be considered operations, which are considered operational clarification needs and which are considered normal intelligence gathering activities (so-called 'day-to-day business').

5.2.5 Resources

In order to be able to ensure effective intelligence operations, it is essential that resources are used expediently.

The OA-IA conducted the following audit in this area in 2020:
- **20-14 Management of suppliers (FIS and EOC)**

20-14 Management of suppliers(FIS and EOC)

The focus of this audit was on the external procurement of goods and services for intelligence activities, in particular on the risk of possible data leaks by suppliers. Accordingly, procurement legislation matters were not the focus of the audit and were not addressed. The ownership structure of companies supply intelligence services is an important indicator when it comes to assessing supplier risk. The OA-IA determined that the risk of possible infiltration of a supplier by a foreign intelligence service can be better countered through increased clarification of the company's environment.

5.2.6 Data processing and archiving

The sensitivity of the information handled by intelligence services is high. In addition, the legal requirements are clear, but also complex. Therefore, OA-IA must pay special attention to the legality of information processing.

OA-IA conducted the following audits in this area in 2020:

- **19-19 Data analysis tools in the EOC**
- **20-15 Right of access (FIS)**
- **20-16 Operation, content and use of the IASA information systems (FIS)**
- 20-17 Information system landscape MIS (authorisation management)
- 20-18 Access by the FIS to third-party information systems (Confederation, cantons, foreign countries) (FIS)
- **20-19 Archive (FIS, unannounced audit)**

“In general, there is a good overview of the EOC's data landscape.”

19-19 Data analysis tools in the EOC

This audit was initially launched in December 2019 and consequently not included in the last Annual Report. Completed in 2020, this more exploratory audit allowed the OA-IA to gain a deeper technical and operational insight into the EOC’s data analysis tools. In general, there is a good overview of the EOC’s data landscape. EOC staff are able to initiate appropriate measures in a timely manner to ensure the performance of the IT infrastructure. The audit did not entail any systematic collection of statistical data for managers within the EOC.

20-15 Right of access/Right to information (FIS)

The right of access is a key mechanism of data protection legislation. It allows the data subject to assert his or her rights under data protection legislation. Only those who know whether and what data about them is being processed can have it corrected or destroyed if necessary.[12]

IntelSA provisions regulate the right to information specifically for the area of internal and external security. If the FIS did not implement the right of access in accordance with legislation, it would run the risk of damaging its reputation. Media coverage of FIS reporting to policymakers in 2019 has confirmed this. The OA-IA considers the lawful handling of requests for information by the FIS to be a key element in promoting the public’s trust in the service. It therefore examined the legality and expediency of the information provided by the FIS in Audit 20-15.

Legal requirements for the provision of information

Information provisions[13] in relation to the following FIS information systems is governed exclusively by the Federal Act on Data Protection (FADP[14]):

- ESD (Electronic Situation Display System: used to share information on the control and implementation of security policy measures)
- OSINT portal (Open-source intelligence: provision of data from publicly accessible sources)
- Quattro P (identification of specific categories of foreigners entering or leaving Switzerland)
- GEVER FIS (System for business processing and control) - administrative data
- Storage system within the meaning of Art. 36 para. 5 IntelSA (particularly sensitive data from operational information-gathering measures that cannot be filed in the general systems).
- Storage system within the meaning of Art. 58 IntelSA (storage system for IGMRAs)

The FADP stipulates[15] that the data subject must generally be given information free of charge and in writing within 30 days about all information contained in the data subject’s file. The FIS may also refuse, restrict or delay information disclosures in accordance with the FADP[16] if need be (e.g. to preserve overriding public interests, in particular internal or external security). Data subjects may appeal this decision to the Federal Administrative Court and in second instance to the Federal Supreme Court.

[12] Federal Council Dispatch of 23 March 1988 on the Federal Data Protection Act (BBl 1988 II 452)

[13] Art. 63 para. 1 IntelSA
[14] SR 235.1
[15] Art. 8 FADP
[16] Art. 9 FADP

For the following information systems, the deferment of provision of information is governed by IntelSA[17]:

- IASA FIS (integral analysis system)
- IASA-GEX FIS (integral analysis system for violent extremism)
- INDEX FIS (personal and organisational identification and filing system for cantonal intelligence services)
- ISCO (Information System Communications Reconnaissance: Control and Management of Radio and Cable Communications)
- Residual data storage (data not allocated to another system)
- GEVER FIS (System for Business Processing and Control) - intelligence data

For these information systems, the FIS shall defer the provision of information if there are overriding interests in confidentiality, which must be justified in the files in connection with:

- the fulfilment of a task under Art. 6 IntelSA; or
- a criminal prosecution or other investigative proceeding; or
- because of overriding interests of third parties; or
- if no data is processed about the data subject.

The FIS shall notify the person making the request of the deferment, stating the legal remedies. If the person is not satisfied with the information, he or she may contact the Federal Data Protection and Information Commissioner (FDPIC).

Implementation of these legal requirements in practice

In practice, the FIS usually defers the provision of information concerning personal data when the data in question relates to sensitive intelligence areas:

Year	Total requests	Information provided	Information disclosure deferred
2019	853	73	746
2020 (until 22 Oct. 2020)	527	16	444

The FIS adapted its directives concerning the provision of information in order to satisfy these legal requirements[18], as recommended by the CDel[19]. It then focused on establishing internal procedures, which had not previously been described in detail and therefore could have resulted in different handling of information requests. The OA-IA recommended that certain adjustments be made to these guidelines as soon as they come up for revision.

The FIS had also developed the practice of giving priority to information requests from politicians and journalists. The answers were given more quickly and in greater detail than to requests made by other parties. In the opinion of the OA-IA, this practice violates the constitutionally guaranteed requirement of equal handling of all information requests. It therefore recommended that this practice be changed immediately.

“In practice the FIS defers the provision of information.”

[17] Art. 63 para. 2 IntelSA

[18] Guidelines on the handling of information requests relating to information and storage systems of the Federal Intelligence Service (FIS) dated 30 October 2020.
[19] Recommendation 4 BBl 2020 3055.

“In the opinion of the OA-IA, this practice violates the constitutionally guaranteed requirement of equal handling of all information requests.”

The OA-IA was shown the database queries in each information system by the person in charge. For the duration of the audit, the OA-IA was given temporary access to the information systems so that it could perform database queries independently. In 20 sample checks, the entries sent to the applicants and documented in the GEVER information system were compared with the hits from our own database queries. This check did not reveal any discrepancies.

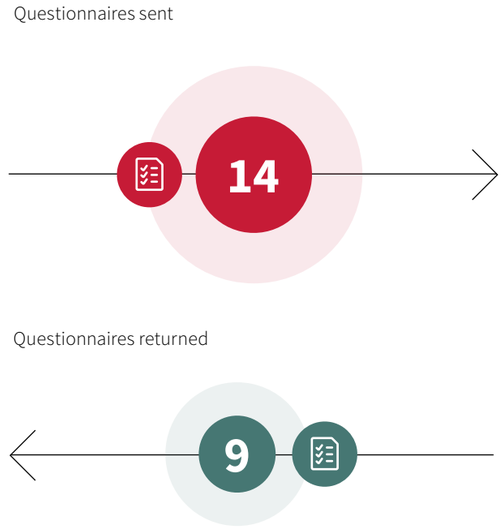
Although this practice with regard to deferrals is lawful, the OA-IA doubted whether this practice was expedient. The legal basis already shows that information disclosure is a very complex matter that requires a correspondingly high level of resources on the part of the FIS. Furthermore, in view of the large number of information requests in recent years, processing an application twice in the case of a deferred information disclosure creates an even greater administrative burden. On the other hand, it can be assumed that most citizens will not accept delayed information disclosure and - understandably - will perceive such decisions as a lack of transparency.

In order to obtain an external perspective, the OA-IA also sent a questionnaire to 14 individuals who had submitted an information request. In selecting the addressees, the OA-IA limited itself to information requests that were examined in greater depth as part of the sample. The OA-IA received eight questionnaires from the fourteen people that had been asked to take part in the survey and one of the respondents answered the questions over the phone.

The following questions were asked:

- Was your information request answered within 30 days? If not, did the FIS notify you of the delay in processing your request?
- How would you rate the level of clarity of the letter received from the FIS?
- Are you satisfied with the answer? Please give reasons for your answer.
- Are you clear about the subsequent procedure that will be followed to process your information request?
- Do you have any other comments on your information request?

Although respondents were unhappy with the long waiting time before receiving a reply from the FIS, they all received notification that there was going to be a delay in the reply.



Respondents were not explicitly negative in their feedback on the clarity of the reply letter. However, most of the citizens were annoyed at having received a letter informing them that information disclosure would be delayed. And in some cases, they viewed this answer as ‘not providing information’. In one case, the person requesting information was satisfied with the feedback given by the FIS because the answer given was that the FIS systems did not have any file with data about the person in question. De facto, however, this person was communicated a deferral and not a Non-listing.

Some respondents complained that the information received was not satisfactory because after a long wait it was still not clear whether the FIS was processing data on the person or not. The respondents also expected more comprehensive information (e.g. what type of data was processed in the individual information systems and how long it was kept for).

Even though the feedback from the questionnaires was by no means representative, the perception of the respondents surveyed coincided with that of the OA-IA. A simple explanation of why the FIS delays information disclosures even in the case of a response indicating that the person’s data was not being processed in FIS databases would improve the general sense of understanding among the population. For applicants without legal expertise, acceptance would probably be increased if, instead of references to legal articles, information in layman’s terms were provided directly in the reply (e.g. information on the different data categories or on retention periods in the information systems).

20-16 Operation, content and use of IASA information systems (FIS)

Each year, OA-IA audits one of the FIS’s information systems. In 2020, IASA was included in the audit plan for this purpose. IASA is the central information system of the FIS and is used to gather, analyse and assess all data flowing into the FIS. This audit examined whether the operation, use and content of this data are lawful and expedient.

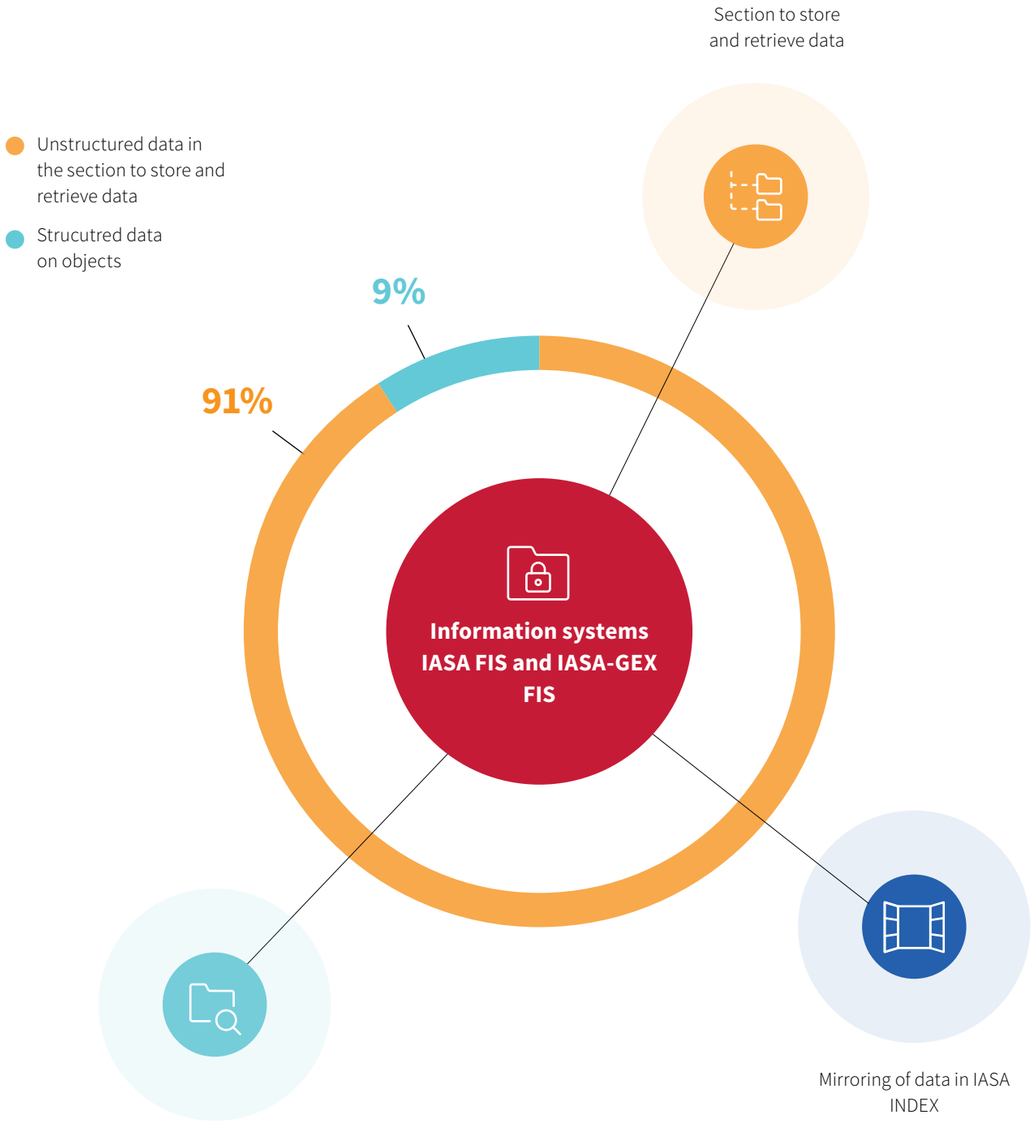
The term IASA broadly refers to three information systems: IASA FIS, IASA-GEX FIS and IASA INDEX, which the FIS is authorised to operate in order to fulfil its tasks. IASA FIS contains data on terrorism, prohibited intelligence activities, non-proliferation and attacks on critical infrastructure. Data on violent extremism are processed separately in IASA-GEX FIS. Finally, IASA INDEX mirrors parts of the recorded data so that agencies outside the FIS (for example, cantonal police under IntelSA provisions and the Federal Office of Police fedpol) can determine whether the FIS is processing data on a person, an object or an event. The latter are only able to see whether or not there is a hit. If necessary, these authorities can then make more detailed enquiries with the FIS.

The information systems IASA FIS and IASA-GEX FIS each have a section that is used to store and retrieve data and an analysis and situation update application used to enter, process, assess and analyse data. The storage and retrieval section contains unstructured data. They are filed unprocessed after a filing check, but can be retrieved at any time by using a search engine. Unstructured data accounts for roughly 91% of the data contained in IASA.

The data entered into the analysis and situation update application are cross-referenced to a person, an object or an event – i.e. arranged in a meaningful manner – and thus form the basis of the FIS structured knowledge base. In addition to the filing check, data also undergo in-depth examination during data entry and therefore have a longer retention period than the unstructured data. Structured data on persons are also checked at regular intervals. About 9% of the data in IASA is structured data.

Based on the audit procedures performed, the OA-IA concluded that the operation and use of IASA FIS, IASA-GEX FIS and IASA INDEX are fundamentally lawful and expedient.

That said, the OA-IA feels that it is not the operation and use of the above-mentioned information systems that poses the greatest risks, but rather the legality of the unstructured data



"The OA-IA was surprised by the sheer volume of documents kept in these archives."

contained in them. The FIS has recognised that there is an urgent need for action in this area and is in the process of taking appropriate measures.

Unannounced Audit 20-19 Archive (FIS)

The audit procedures were carried out on site over a two-day period. The original plan was to conduct the audit shortly after the media reports came out on the secret archives relating to the Crypto AG case. It was not possible for the OA-IA to gain access to an external site (the command facility, which housed a portion of FIS archives) entirely unannounced as this facility first had to be powered up and put into operation. This required a lead time of several days. The OA-IA requested the access logs for the facility over this period to make sure that no one had entered the premises in the meantime.

The FIS had to assign a large number of staff to assist the OA-IA in its audit activities. It did this as a matter of course and provided OA-IA auditors with full support.

The OA-IA was surprised by the sheer volume of documents kept in these archives. The FIS stores several hundred metres of documents in various locations. These documents date from a time when the FIS was not yet subject to OA-IA oversight. There was only a rough inventory of the contents of these files and archives. At the time of the audit, the FIS had already engaged in discussions with the Federal Archives and had reached an agreement that all documents that were not essential to operations would be handed over to the Federal Archives by the end of 2020. The OA-IA therefore did not see the need to make a corresponding recommendation. The audit findings were enough to elucidate CDel questions.
Unannounced audits are a valuable tool for the OA-IA. It will continue to use them in the future after careful consideration of all the costs and benefits involved.

5.3 Acceptance

In the 2019 Annual Report, the OA-IA discussed its practice of issuing advisory notices to accompany recommendations pursuant to Art. 78 para. 6 IntelSA. There was no explicit basis for OA-IA advisory notices and they were intended as a temporary, methodical means of achieving the desired outcomes. There were two cases where the OA-IA had formulated advisory notices in relation to its audits:

1) where the proposed optimisation measure identified during the audit did not require the direct involvement of the head of the DDPS in order to be implemented but rather could be carried out at a lower operational level (e.g. policy on allowing cell phones at meetings where confidential information is discussed).
2) where findings were incidental and not directly related to the given audit but were nevertheless relevant to a certain degree.

This practice had initially been introduced in consultation with the predecessor of the current head of the DDPS. The implementation of the advice notices was not verified by the OA-IA.

At the request of the current head of the DDPS and in the absence of an explicit legal basis, the OA-IA will now refrain from formulating advisory notices for all audits from 2020 onwards. However, the facts will continue to be described in the text of audit reports. In the evaluation, however, only recommendations will be made if objectively necessary.

In the course of their work, the auditors were received by all audited entities in a constructive and professional manner. They were given access to the documents and information systems needed to carry out the audit assignments. The interviewees were available to the auditors. The interviews could be planned and conducted in a timely manner and additional questions were answered as quickly as possible.

5.4 Controlling of recommendations

Verification of implementation of recommendations is not explicitly regulated by IntelSA. In agreement with the DDPS and the audited services, it was agreed that the latter would inform the DDPS in writing of progress made towards implementation of OA-IA recommendations and that the OA-IA would receive a copy of those progress updates. In addition, a meeting was held in the middle of the year with all audited services and in the presence of a DDPS representative to take stock of the current state of implementation of recommendations. In that meeting, the reporting process was confirmed and supplemented (e.g. to include requests for deadline extensions). These meetings will be repeated at least once a year in the future.

In 2020, 56 recommendations were scheduled for formal implementation. Of this total, the OA-IA received confirmation of implementation for 12 recommendations. In the area of information gathering/operations, the recommendations reported as having been implemented are reviewed in audit 20-11. Around half of the recommendations were slated for implementation by 31 December 2020. At the time this Annual Report went to press, the OA-IA had not received confirmation of implementation of those recommendations. From 2018, only recommendations with a current deadline are still pending.

The case of implementation of a recommendation from Audit 18-11 (overview of measures to reduce risks in the MIS) is worth mentioning. On 28 August 2018, the OA-IA recommended that consideration be given as to whether the Service for Preventive Protection of the Armed Forces (DPSA) should be included in OA-IA oversight in the revised draft of the Federal Act on the Armed Forces and Military Administration (ArmA)[20].

DPSA's role is to protect the Armed Forces from espionage, sabotage and other unlawful acts. The aim is to identify threats in good time and take preventive measures to prevent damage to the Armed Forces. The activities of the DPSA are carried out in close cooperation with federal and cantonal authorities and reports are submitted to Armed Forces command, to troops and to the responsible national, cantonal and, if applicable, multinational authorities and commands. The legal basis for the DPSA can be found in Article 100 ArmA. In organisational terms, the DPSA is combined with the MIS and report to one chief.

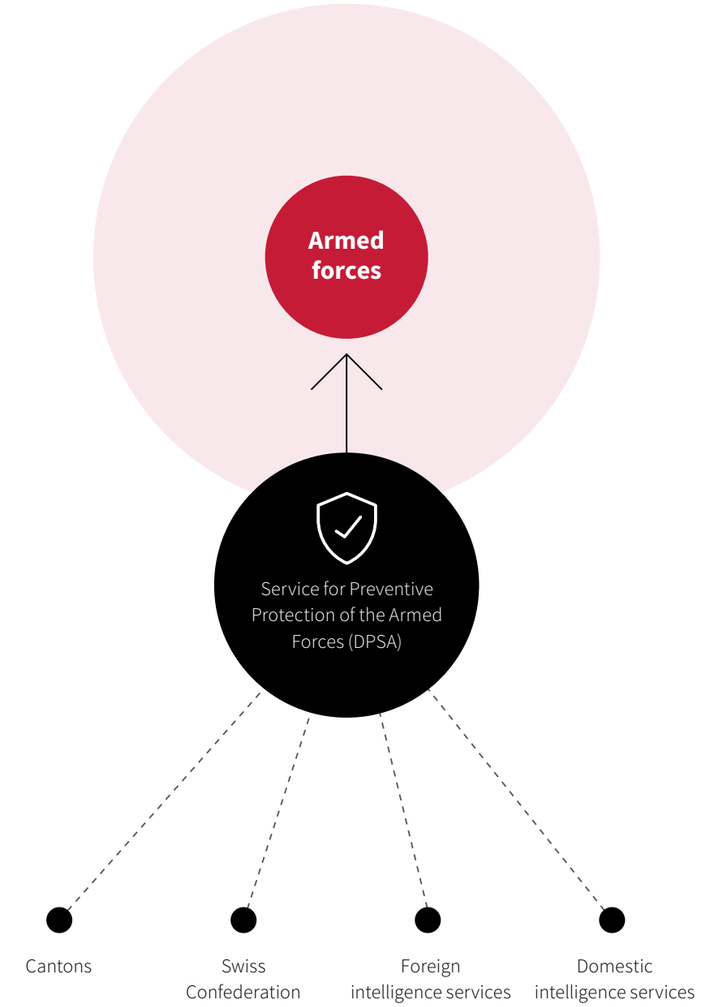
To carry out its tasks, the DPSA has access to various information systems containing personal data. The current revision of the Federal Act on Military Information Systems (MISA)[21] is intended to provide an adequate legal basis for this. According to the revised draft, the DPSA maintains a very extensive database of personal data on military personnel. This database is intended to ensure the preventive protection of the Armed Forces. The DPSA can also obtain information from foreign or domestic intelligence services. In light of this, the OA-IA is of the opinion that the DPSA probably processes even more personal data on Swiss citizens for the purpose of preventive protection of the Armed Forces than the MIS itself. However, like the MIS, the DPSA is not subject to independent oversight.

After initially responding favourably to the OA-IA's recommendation, the MIS issued a statement in August 2018, referring only to the matter of responsibility for implementation. This letter was then followed up by another letter from the Chief of the Armed Forces (CAF) dated 1 May 2020, stating without further explanation that the OA-IA's recommendation had been discussed in the meantime and that from the Armed Forces' perspective there was currently no need for OA-IA oversight to be extended to include the DPSA. The Head of the DDPS took note of the CAF's letter on 2 June 2020. When asked to clarify its position on the matter, the MIS refrained from discussing DPSA processing of personal data. The OA-IA's recommendation was therefore taken into consideration and the DPSA will continue not to be subject to independent oversight.

[20] SR 510.10

[21] SR 510.91

Data processing by the DPSA



6. Insights from inside

6.1 Coronavirus

The first wave of the federal government's coronavirus response hit OA-IA after the first audits began in 2020. So there was a worklist available. The OA-IA offered its availability to other agencies via the General Secretariat (GS) of the DDPS to assist in handling this extraordinary situation. This offer was not taken up.

Measures allowing staff to work from home were introduced and this has basically worked well. However, satisfying data protection requirements with this form of work has been somewhat of a challenge. Moreover, the loss of spontaneous and informal exchanges among members of the audit team has been one of the most serious consequences of the shift to working from home. This was partly compensated for by regular one-on-one telephone conversations. The efforts made in the first two years to consolidate teamwork paid off and allowed work to continue smoothly. Due to security concerns, no video conferences could be held in relation to oversight activities.

6.2 Personnel and continuing training

OA-IA still has a staff of ten (9.1 FTEs). A French-speaking lawyer left us in the middle of the year. Her replacement, who also speaks French, began work on 1 August 2020.

Continuing training opportunities were also limited because of corona-related restrictions.

Only one event on the cyber topic was held. Continuing training in survey techniques and the second cyber topic event had to be postponed, as did an event that would have covered security policy. Webinars were attended sporadically. In general, most of the team's training had to be replaced by self-study.

6.3 Archiving

As a federal authority, the OA-IA must submit its documents to the Swiss Federal Archives (SFA). The OA-IA classification system, its evaluation and the associated regulations were approved by the SFA during the reporting year. The approval process has thus been completed. In consultation with the SFA, the OA-IA can now begin delivering its documents that are worth archiving.

6.4 Strategy

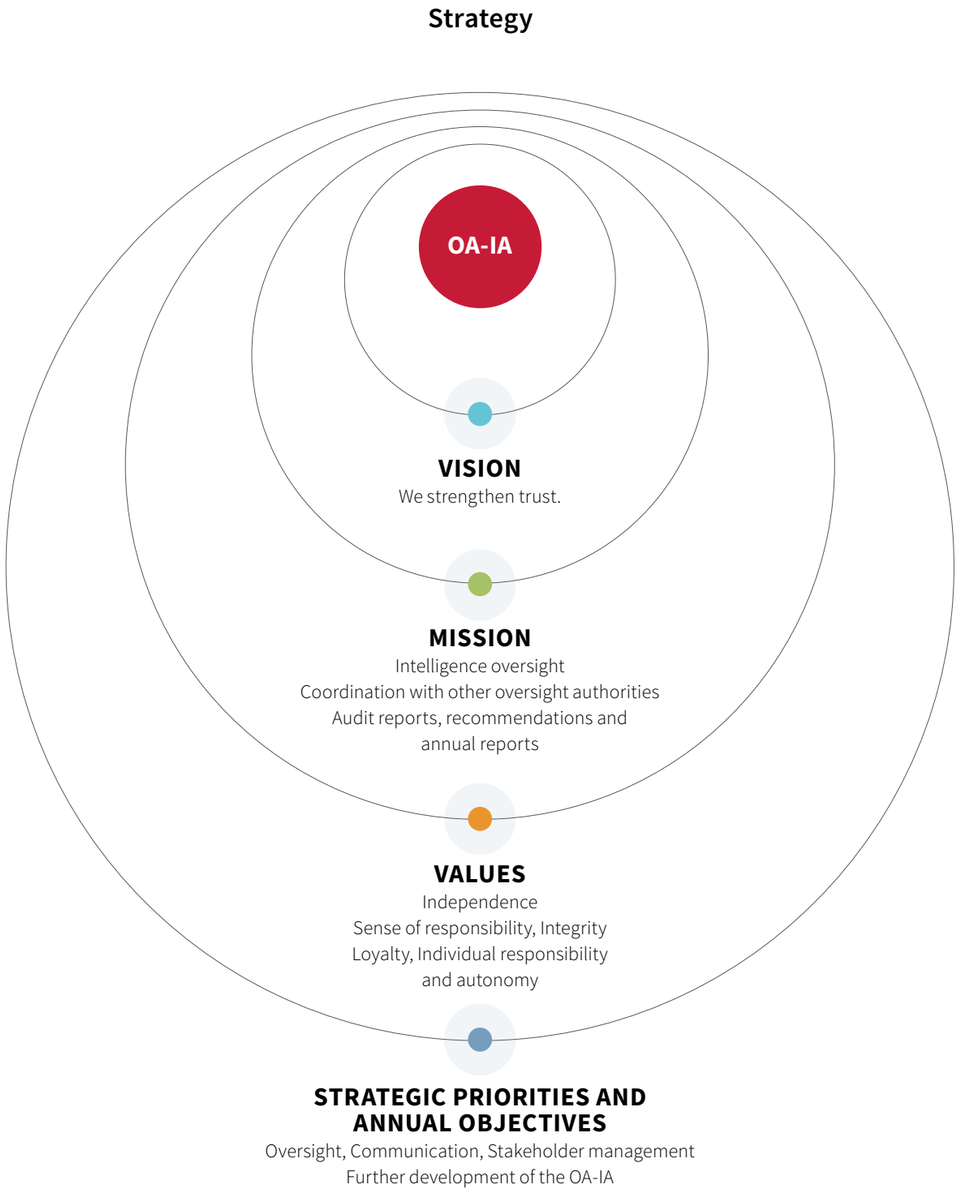
One of the OA-IA's annual objectives was to develop its own strategy. Its vision, mission statement, values and strategic priorities were jointly formulated in three workshops and in written consultations. The OA-IA's strategy will remain in place until 2024 and thus corresponds to the term of office of the head of the OA-IA.

6.5 Freedom of Information Act (FOIA)[22]

OA-IA received two requests for access to official documents in the reporting year. The first request was granted in full. It concerned access to two OA-IA internal documents. A partially redacted document was provided in response to the second request. In doing so, the OA-IA followed its policy of building trust in intelligence activities through transparency wherever possible.

[22] SR 152.3

"Measures allowing staff to work from home worked well but have their limits due to information protection requirements."



7. Coordination

The OA-IA must coordinate its activities with those of parliamentary, federal and cantonal oversight bodies. However, this coordination - especially in matters of personal exchange - was also strongly influenced by the Corona pandemic and the associated restrictive measures in 2020. Consequently, meetings with the Federal Administrative Court (FAC), the Swiss Federal Audit Office (SFAO), the Supervisory Authority for the Office of the Attorney General of Switzerland (SA-OAG), the Post and Telecommunications Surveillance Service (PTSS) and the DDPS Internal Audit Service (DDPS IAC) could not take place as planned, or could only take place to a limited extent.

7.1 National contacts

Control Delegation (CDel)

The CDel invited the head of the OA-IA to attend a hearing on 1 May 2020. At this hearing, OA-IA management informed the CDel about an oversight letter submitted by the Control Committee (CC) of the Canton of Bern regarding the OA-IA's report for Audit 19-7 CIS Bern, the 2019 OA-IA's Annual Report 2019 and Audit 20-19 Archive.

National Council Security Policy Committee (SPC-NC)

On 17 October 2020, the head of OA-IA was invited to a meeting of the SPC-NC. At this meeting, the 2019 Annual Report was presented and discussed. This was followed by a Q&A session.

Federal Council Security Committee (FCSC)

Each year, OA-IA staff attend a meeting of the Federal Council Security Committee (FCSC) to share information with representatives of the GS of the Federal Department of Foreign Affairs (FDFA), the Federal Department of Justice and Police (FDJP) and the DDPS. In 2020, this meeting was held on 18 August.

Federal Administrative Court (FAC)

The OA-IA staff also meets with FAC representatives to share information. The first 2020 meeting was held on 15 July. Technical questions regarding IGMRAs and cable exploration were discussed – separately from the operations. The second meeting planned for December had to be postponed.

Independent Control Authority for Radio and Cable Communication (ICA)

On 17 June 2020, the ICA invited an OA-IA representative to attend a workshop on cable exploration. In the first part of this workshop, FIS staff spoke about current and future organisational issues relating to cable exploration. In the second part, EOC staff provided more technical details to elaborate on the explanations given by FIS staff. In the third part, there was finally an exchange of opinions among those in attendance. The aim of the meeting was to ensure that all the agencies involved had the same level of knowledge about problems and modalities in the area of cable exploration.

On 4 September 2020, the President of the ICA and the Head of OA-IA met for an informal exchange. Among other things, they discussed the planned FIS review with regard to oversight authorities.

One OA-IA staff member participated as an observer in each of three ICA oversight events. This helped to facilitate the exchange of information.

Meeting with the cantonal oversight bodies

After the first meeting held back in 2018, the OA-IA decided that 2020 would be a good opportunity to once again meet with cantonal bodies responsible for oversight of intelligence activities. A follow-up meeting and an exchange of experiences had been explicitly requested by many cantons. However, no physical meeting could be arranged in 2020 due to the COVID-related restrictions and online meetings to discuss intelligence topics could not be held due for security reasons. The event therefore had to be postponed until later.

Inquiries from citizens

The OA-IA received eleven inquiries from citizens in 2020.

The head of the OA-IA met with the following people in 2020:

- Head of the DDPS (20 January 2020, 22 September 2020)
- Secretary General of the DDPS (25 February 2020, 19 August 2020, 11 December 2020)
- Director of the FIS (19 January 2020, 26 February 2020, 6 April 2020, 4 June 2020, 29 June 2020, 3 September 2020, 3 December 2020)
- Head of the MIS (15 January 2020, 28 April 2020, 23 June 2020, 28 October 2020)
- Head of the EOC (13 January 2020)
- FDPIC staff (25 February 2020)

7.2 International contacts

The scope of OA-IA audits of Switzerland's intelligence activities is limited to the country's borders.

Currently, there is no legal basis that would enable the OA-IA to engage in joint oversight activities with other foreign oversight bodies. Nevertheless, the sharing of methods and experiences has proven to be very valuable.

However, due to the Corona-related travel restrictions - apart from a meeting in Oslo in January - personal exchanges with other European intelligence oversight authorities had to be dispensed with.

Also in January, the OA-IA was invited to the anniversary of Standing Committee I[23], the Belgian regulatory body.

Oslo, 20 and 21 January 2020: Meeting of the Intelligence Oversight Working Group (IOWG)

Representatives of intelligence oversight authorities from Belgium, Denmark, the Netherlands, Norway, England, Sweden and Switzerland met for an exchange of best practices. On this occasion, staff from the Norwegian oversight authority presented working tools and discussed them in the plenary. The legal basis of the oversight authorities for a possible international oversight activity was also discussed.

[23] Standing Intelligence Agencies Review Committee

8. A view from outside (carte blanche)

The annual report also includes an external perspective. In keeping with the theme of control and oversight, André Duvillard presents his personal view of things.

Efficient oversight thanks to clear framework

1. The concept of control

The concept of control runs like a golden thread through the OA-IA's Annual Report. My thoughts on this subject stem from my experience as SSN Delegate, having closely observed recent challenges in the area of internal security and the efforts made by the various actors to address them.

The Larousse dictionary defines control as 'controlling something or someone, determining the condition or situation on the basis of a set of standardised criteria'.

The intelligence services in general are characterised by the secrecy that surrounds their organisation, their activities and even the nature of these activities, which move between myth and reality. The world of intelligence services arouses curiosity, unsettles people or leads to misconceptions – and often the colloquial term 'secret services' is used in reference to them. For the layperson, the general impression is that intelligence activities are not subject to any oversight whatsoever, and this impression is certainly reinforced by the fact that intelligence services often resort to methods and procedures that are then hidden beneath the veil of national interest and hence the necessity of a heightened degree of secrecy.

These peculiarities may lead one to believe that the intelligence services are hardly subject to binding oversight processes due to the special nature of their tasks. In the Swiss context, however, this is not true at all. The OA-IA's first Annual Report from 2018[24] lists no fewer than ten bodies responsible for overseeing the intelligence services. No other state activity is examined in such detail. But the density of oversight is simply explained by the extremely sensitive nature of the tasks and by the means available to the services to carry them out.

The high density of oversight bodies confirms that in a democratic state there are by definition no secret activities in the literal sense, i.e. activities that take place without anyone else knowing about them.

André Duvillard (*1960)
André Duvillard was appointed as common delegate for the Swiss Security Network (SSN) by the Confederation and the cantons in 2012. He moderates the dialog between the Confederation and the cantons and is supported by an office.

André Duvillard graduated in law from the University of Neuchatel in 1987. He then worked as a delegate of the International Committee of the Red Cross (ICRC) in Iraq, Israel and Lebanon. From 1991-1997, he worked for the Parliamentary Services as Secretary of the respective Security Policy Committee (SPC) of the National Council and the Council of States. Between 1997-2012, he worked for the Neuchatel cantonal police as deputy commander and, from 2005, as police commander.

[24] https://www.ab-nd.admin.ch/en/jahresbericht-ab-nd.html

2. Ensuring accountable intelligence within the framework of democratic governance[25]

This important oversight activity must ensure the proper functioning of the various state institutions responsible for security and ultimately help to improve the level of security of the country and its citizens. It must also guarantee respect for democratic principles that prevail in a state governed by the rule of law.

The effectiveness of oversight of intelligence services can therefore only be ensured if certain general conditions are met and also implemented by the actors concerned.

Awareness of threats

The main tasks that the FIS carries out on behalf of the authorities are prevention and situation assessment. These tasks justify providing the FIS with specific means and competences to serve as the 'country's first line of defence', as the current FIS Director often puts it.

Here, political oversight (by Parliament and the Federal Council) is crucially important. It is up to politicians to assess the perceived threat and the expediency of measures taken to counter that threat and ultimately decide what resources and competences are required to do so.

Freedom of action in the fulfilment of tasks

The FIS's early detection and forecasting capabilities play a decisive role in the fulfilment of its tasks. The FIS must recognise and assess threats in good time so that it can then take the necessary precautionary measures.

But the world of intelligence is by definition not binary, it is not all black or white. There are many shades of grey in between, and if one is objective, one has to acknowledge that this activity sometimes necessarily means navigating murky waters.

The great difficulty is to give the intelligence service sufficient freedom of action to fulfil its tasks while at the same time respecting the democratic principles of the rule of law. This delicate balance is what makes oversight activity so challenging and sometimes leads to differing views between the oversight bodies and the intelligence service.

[25] Geneva Centre for Security Sector Governance (DCAF), Geneva, 'Intelligence Oversight – Ensuring accountable intelligence within a framework of democratic governance', series of security sector reform backgrounders (Geneva: DCAF, 2017).

Technological advances

The development of information and communication technologies opens up considerable possibilities in the area of intelligence gathering. This development is taking place both rapidly and with a certain complexity. Consequently, control can only be effective if the oversight bodies are aware of the technological possibilities and the associated risks. This requires a lot of work to provide and share information and give explanations. This is because decisions made based on a lack of understanding of a given subject matter are bound to be incomplete or inappropriate.

Complementarity and coordination of oversight activities

As mentioned above, intelligence activities are subject to extensive oversight by different bodies and at different levels. The challenge is not so much to determine the appropriate number of audits, but to ensure a coherent approach by the oversight bodies. For despite the precise legislative framework for oversight, there is a risk of duplication and invariably different assessments.

Consequently, coordination must be handled in a way that everyone can agree with. Ideally, this should be based on the principles of coherence and efficiency. In this manner, those subject to oversight (namely the intelligence services) are more likely to accept oversight measures.

In summary, it can be said that the oversight of intelligence activities is now part of everyday life in our democratic societies. In Switzerland, oversight has been greatly expanded since the end of the 1990s following various reforms in structures and allocation of powers, but also in the wake of events such as the secret files scandal.

The creation of the OA-IA in 2017 was another important milestone in the development of oversight activities. Today, the OA-IA plays an important role in the process of monitoring intelligence activities, which collectively forms a complex clockwork. In the coming years, fine-tuning will undoubtedly take place to make it a reliable precision instrument.

9. Key figures as of 31 December 2020 [26]

Staff

1 January 2020	**10**
31 December 2020	**10**
Departures	**1 (1)**

Audits

Planned	**18 (21)**
Unannounced audits	**1 (0)**
Audits conducted	**17 (19)**

Interviews

102 (119)

Budgeted workforce

10 (10)

Recommendations

55 (63)

Advisory notices:

Are no longer formulated

10. Appendix

10.1 2020 Audit Plan

No.	Name of audit	Agency audited
Strategy and Planning		
20–1	Change management	a) FIS[1] / b) MIS[2] / c) EOC[3]
20–2	Additional resource requirements	FIS
Organisational Aspects		
20–3	Allocation of powers and responsibilities between FISA[4] - MIS	FIS / MIS
Cooperation		
20–4	Audit of Cantonal Intelligence Service (CIS) St. Gallen	FIS / CIS
20–5	Audit of CIS Zurich	FIS / CIS
20–6	Audit of CIS Ticino	FIS / CIS
20–7	Audit of CIS Solothurn	FIS / CIS
20–8	Audit of CIS Fribourg	FIS / CIS
20–9	Partner services	a) FIS / b) MIS
20–10	Cooperation with partners at federal level	FIS
Procurement		
20–11	Operations (incl. information-gathering measures requiring authorisation)	FIS
20–12	Human intelligence (HUMINT)	FIS
20–13	Operational clarification needs	FIS
Resources		
20–14	Management of suppliers	a) FIS / b) EOC
Processing / Data Storage		
20–15	Right of access	FIS
20–16	Operation, content and use of IASA information system[5]	FIS
20–17	Information systems used by MIS (authorisation management)	MIS
19–18	Access to/from third-party information systems (Confederation, Cantons, foreign agencies, law enforcement agencies)	FIS

[1] Federal Intelligence Service
[2] Military Intelligence Service
[3] Electronic Operations Centre
[4] Federal Intelligence Service, Analysis Division
[5] Integrated analysis system of FIS

10.2 List of abbreviations

AG
Aktiengesellschaft (public limited company)

ArmA
Federal Act on the Armed Forces and the Military Administration (SR 510.10)

Art.
Article

BBl
Federal Gazette

CC
Control committee

CCPCS
Conference of Cantonal Police Commanders of Switzerland

CDel
Control Delegation

C-facility
Command facility: used to house commanding officers of large divisions of the Swiss Armed Forces

CIS
Cantonal intelligence services

CORONA
Short form for a family of viruses

CYBER
Word used to describe data platforms and the Internet.

DCAF
Geneva Centre for Security Sector Governance

DDPS
Federal Department of Civil Protection, Defence and Sport

DPSA
Service for Preventive Protection of the Armed Forces

Data server under Art. 36 Para. 5 IntelA
FIS data server containing operational intelligence data of a particularly sensitive nature, which therefore cannot be stored on the general data servers.

Data server under Art. 58 IntelA
FIS data server used to store data relating to information gathering measures requiring approval

e.g.
For example

EOC
Electronic Operations Centre

ESD
Electronic Situation Display system of the FIS

FAC
Federal Administrative Court

FADP
Federal Data Protection Act (SR 235.1)

FCSC
Federal Council Security Committee

FDFA
Federal Department of Foreign Affairs

FDJP
Federal Department of Justice and Police

FDPIC
Federal Data Protection and Information Commissioner

FIS
Federal Intelligence Service

FOIA
Federal Act on Freedom of Information in the Administration (SR 152.3)

FTE
Full-time equivalent, unit used to assess working time

GEVER
Electronic records and process management used by the Federal Administration

GS
General Secretariat

HUMINT
Human intelligence, information gathering through human sources

IASA FIS
Integral analysis system of the FIS

IASA-GEX FIS
Integral analysis system of the FIS for matters pertaining to violent extremism

ICA
Independent Control Authority for Radio and Cable Communication

IGMRA
Procurement measures subject to approval

INDEX FIS
Information system of the FIS, used to identify people and organisations and serves as a data server for cantonal intelligence services.

IntelSA
Federal Act on the Intelligence Service (SR 121)

IR DDPS
Internal Revision DDPS

ISCO
The FIS information system is used for communications reconnaissance

MIS
Federal Military Intelligence Service

MISA
Federal Act on Military Information Systems (SR 510.91)

NAP
National Action Plan to Prevent and Counter Radicalisation and Violent Extremism

NDBA
Analysis Directorate of the FIS

OA-IA
Independent Oversight Authority for Intelligence Activities

OSINT-Portal
Open Source Intelligence, intelligence information derived from publicly available sources

Para.
Paragraph

PTSS
Post and Telecommunications Surveillance Service

SA CIS
Specialist application of the cantonal intelligence services

SA-OAG
Supervisory Authority for the Office of the Attorney General

SFA
Swiss Federal Archives

SFAO
Swiss Federal Audit Office

SPC-N
National Council Security Policy Committee

SR
Classified Compilation of Swiss legislation

SVS
Swiss National Security Network

Quattro P
Information system used by the FIS to identify special categories of foreigners entering and leaving Switzerland

VIGIPOL
Fribourg Cantonal Police Headquarters

Independent Oversight Authority
for Intelligence Activities
Maulbeerstrasse 9, 3003 Bern
Phone +41 58 464 20 75
www.ab-nd.admin.ch