EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Audit de la surveillance

Autorité de surveillance indépendante des activités de renseignement

CDF-23117 | Prises de position incluses | 13 novembre 2023

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Contrôle fédéral des finances (CDF) Monbijoustrasse 45 3003 Berne Suisse
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	502.23117
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch + 41 58 463 11 11
Abdruck Reproduction Riproduzione Reprint	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

Table des matières

Audit de la surveillance
Autorité de surveillance indépendante des activités de renseignement

L'essentiel en bref

Créée en 2017, l'Autorité de surveillance indépendante des activités de renseignement (AS-Rens) est une unité décentralisée de l'administration fédérale qui a pour tâche de contrôler les activités de renseignement quant à leur légalité, leur adéquation et leur efficacité. Le personnel de l'AS-Rens a connu une forte fluctuation en 2021 et 2022. Une nouvelle directrice a pris ses fonctions en juillet 2022, désormais l'effectif de neuf collaborateurs est quasi au complet (état août 2023). Le budget de l'AS-Rens se monte à 2,3 millions de francs en 2023, les dépenses de personnel représentent plus de 80 % des charges de fonctionnement.

Le Contrôle fédéral des finances (CDF) a effectué un audit auprès de l'AS-Rens dans le but de vérifier l'application de la loi sur le renseignement, du règlement interne et des processus. Les résultats sont positifs. Le cadre légal est respecté et l'organisation est adéquate. Toutefois, le CDF recommande à l'AS-Rens de procéder à plusieurs améliorations pour renforcer l'efficacité de sa surveillance.

Développer l'évaluation des risques

Le processus d'analyse de risques se concentre sur les six domaines de surveillance définis par l'AS-Rens. Tous les collaborateurs de l'AS-Rens participent à la définition et à l'appréciation des thèmes et des risques pour établir le plan annuel des inspections. Pour mieux évaluer les risques et assurer une vue d'ensemble, l'AS-Rens devrait disposer d'une cartographie des risques globaux liés aux domaines du renseignement, mais aussi effectuer une appréciation des risques pour chaque entité soumise à sa surveillance. D'autres critères de risques pourraient être définis, comme ceux relatifs au développement futur du domaine du renseignement ainsi que ceux liées à l'organisation des tâches, à la complexité de la base légale ou à la transversalité des activités.

Adapter le manuel d'inspection et rendre plus lisible les rapports

Le manuel d'inspection offre une grande marge de manœuvre dans son application. Il devrait être adapté pour garantir une unité de doctrine, assurer une meilleure traçabilité de la documentation et mieux définir le processus d'assurance qualité.

La destinataire finale des rapports est la cheffe du Département fédéral de la défense, de la protection de la population et des sports. Les rapports sont en général trop détaillés et par conséquent relativement longs. Le fil rouge entre les constatations, les appréciations et les recommandations est parfois difficile à suivre. Le CDF recommande d'améliorer leur lisibilité.

Revoir la sécurité des systèmes informatiques

Bien que consciente des risques liés à son infrastructure informatique et au traitement de l'information, l'AS-Rens devrait effectuer une revue critique des documents de sécurité de ses propres systèmes. Pour évaluer pleinement les risques, elle devrait exiger et consulter les documents de sécurité informatique développés par ses fournisseurs de prestations et par les entités propriétaires des systèmes utilisés dans le cadre des inspections. Les documents devraient être adaptés et les incohérences corrigées.

Prüfung der Aufsicht

Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten

Das Wesentliche in Kürze

Die 2017 gegründete unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten (AB-ND) ist eine dezentrale Einheit der Bundesverwaltung, deren Aufgabe darin besteht, nachrichtendienstliche Tätigkeiten auf ihre Rechtmässigkeit, Zweckmässigkeit und Wirksamkeit hin zu überprüfen. In den Jahren 2021 und 2022 war die Fluktuation des Personals der AB-ND hoch. Im Juli 2022 übernahm eine neue Direktorin die Leitung, nun ist der Personalbestand mit neun Mitarbeitenden quasi vollständig (Stand August 2023). Das Budget der AB-ND für 2023 beträgt 2,3 Millionen Franken, die Personalausgaben machen mehr als 80 Prozent des Funktionsaufwands aus.

Die Eidgenössische Finanzkontrolle (EFK) hat bei der AB-ND ein Audit durchgeführt, um zu überprüfen, ob das Nachrichtendienstgesetz, die Geschäftsordnung und die Prozesse eingehalten werden. Die Ergebnisse sind positiv. Der rechtliche Rahmen wird eingehalten und die Organisation ist angemessen. Die EFK empfiehlt der AB-ND jedoch, mehrere Verbesserungen vorzunehmen, um die Wirksamkeit ihrer Aufsicht zu erhöhen.

Risikobewertung weiterentwickeln

Der Prozess der Risikoanalyse konzentriert sich auf sechs von der AB-ND festgelegte Aufsichtsbereiche. Alle Mitarbeitenden der AB-ND beteiligen sich an der Festlegung und Bewertung der Themen und Risiken für die Erstellung des Jahresprüfplans. Um die Risiken besser einschätzen zu können und einen Gesamtüberblick zu gewährleisten, sollte die AB-ND über ein Diagramm der Gesamtrisiken in den Nachrichtendienstbereichen verfügen, aber auch eine Risikobewertung für jede von ihr beaufsichtigte Stelle vornehmen. Weitere Risikokriterien könnten festgelegt werden, beispielsweise im Hinblick auf die künftige Entwicklung des nachrichtendienstlichen Bereichs, die Organisation der Aufgaben, die komplexe Rechtsgrundlage oder den Querschnittscharakter der Tätigkeiten.

Prüfungshandbuch anpassen und Lesbarkeit der Berichte verbessern

Das Prüfungshandbuch bietet viel Spielraum bei der Anwendung. Es sollte angepasst werden, um eine *unité de doctrine* sicherzustellen, eine bessere Rückverfolgbarkeit der Dokumentation zu gewährleisten und den Qualitätssicherungsprozess genauer zu definieren.

Empfängerin der Berichte ist die Vorsteherin des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport. In der Regel sind die Berichte zu ausführlich und daher ziemlich lang. Bisweilen ist es schwierig, den roten Faden zwischen Feststellungen, Beurteilungen und Empfehlungen zu finden. Die EFK empfiehlt, die Lesbarkeit der Berichte zu verbessern.

Sicherheit der IT-Systeme überprüfen

Obwohl die AB-ND sich der Risiken bewusst ist, die mit ihrer IT-Infrastruktur und der Informationsverarbeitung einhergehen, sollte sie die Sicherheitsdokumentation ihrer eigenen Systeme einer kritischen Prüfung unterziehen. Zur vollumfänglichen Risikobewertung sollte sie die IT-Sicherheitsdokumentation, die von ihren Leistungserbringern und von den Eigentümern der für die Prüfung verwendeten Systeme entwickelt wurde, einfordern und sichten. Diese Dokumentation sollte angepasst und Unstimmigkeiten sollten korrigiert werden.

Originaltext auf Französisch

Verifica della vigilanza
Autorità di vigilanza indipendente sulle attività informative

L'essenziale in breve

Istituita nel 2017, l'Autorità di vigilanza indipendente sulle attività informative (AVI-AIn) è un'unità decentralizzata dell'Amministrazione federale che svolge controlli sulle attività informative verificandone la legalità, l'adeguatezza e l'efficacia. Il personale dell'AVI-AIn ha subìto forti fluttuazioni negli anni 2021 e 2022. Una nuova direttrice ha assunto le sue funzioni nel luglio del 2022 e l'effettivo, composto di nove collaboratori, è ora quasi al completo (stato: agosto 2023). Il budget dell'AVI-AIn ammonta a 2,3 milioni di franchi nel 2023, le uscite per il personale rappresentano oltre l'80 per cento delle spese di funzionamento.

Il Controllo federale delle finanze (CDF) ha effettuato una verifica presso l'AVI-AIn per accertarsi dell'applicazione della legge federale sulle attività informative nonché del regolamento interno e dei processi. I risultati della verifica sono positivi. Il quadro legale è garantito e l'organizzazione adeguata. Tuttavia, il CDF raccomanda all'AVI-AIn di apportare diversi miglioramenti per aumentare l'efficacia della sua vigilanza.

Sviluppare la valutazione dei rischi

Il processo di analisi dei rischi si concentra sui sei ambiti di vigilanza definiti dall'AVI-AIn. Tutti i suoi collaboratori partecipano alla definizione e alla valutazione dei temi e dei rischi al fine di definire il piano annuale delle ispezioni. Per valutare meglio i rischi e garantire una visione d'insieme, l'AVI-AIn dovrebbe disporre di una carta dei rischi globali legati ai settori dei servizi di informazione, ma anche effettuare una valutazione dei rischi per ciascuna unità sottoposta alla sua vigilanza. Si potrebbero definire altri criteri di rischio, come quelli concernenti il futuro sviluppo del settore dei servizi di informazione nonché l'organizzazione dei compiti, la complessità della base legale o la trasversalità delle attività.

Adeguare il manuale di ispezione e rendere i rapporti più leggibili

Il manuale di ispezione offre un ampio margine di manovra nella sua applicazione. Esso andrebbe adeguato per garantire un approccio uniforme e una migliore tracciabilità della documentazione nonché definire meglio il processo di garanzia della qualità.

Il destinatario finale dei rapporti è il capo del Dipartimento federale della difesa, della protezione della popolazione e dello sport. In generale, i rapporti sono troppo dettagliati e, quindi, relativamente lunghi. Talvolta il filo conduttore tra le constatazioni, le valutazioni e le raccomandazioni è difficile da seguire. Il CDF raccomanda di migliorarne la leggibilità.

Rivedere la sicurezza dei sistemi informatici

Pur consapevole dei rischi correlati alla propria infrastruttura informatica e al trattamento delle informazioni, l'AVI-AIn dovrebbe rivedere in modo critico i documenti di sicurezza dei propri sistemi. Per valutare appieno i rischi, l'autorità dovrebbe richiedere e consultare i documenti di sicurezza informatica sviluppati dai suoi fornitori di prestazioni e dalle unità responsabili dei sistemi utilizzati nel quadro delle ispezioni. I documenti devono essere adeguati e le incongruenze corrette.

Testo originale in francese

Supervision audit
Independent Oversight Authority for Intelligence Activities

Key facts

Established in 2017, the Independent Oversight Authority for Intelligence Activities (OA-IA) is a decentralised unit of the Federal Administration whose task is to review intelligence activities with regard to their legality, appropriateness and effectiveness. OA-IA employee numbers fluctuated significantly in 2021 and 2022. A new director took up her post in July 2022, and the team of nine is now almost complete (as at August 2023). The OA-IA budget for 2023 is CHF 2.3 million, with personnel costs accounting for more than 80% of operating expenses.

The Swiss Federal Audit Office (SFAO) audited the OA-IA with a view to verifying compliance with the Intelligence Act, internal regulations and processes. The results were positive. The legal framework is respected and the organisation is appropriate. However, the SFAO recommended that the OA-IA make several improvements to enhance the effectiveness of its supervision.

Develop risk assessments

The risk analysis process focuses on the six areas of supervision defined by the OA-IA. All OA-IA staff are involved in defining and assessing the topics and risks to be covered in the annual inspection plan. In order to better assess risks and ensure an overall view, the OA-IA should not only have a map of overall risks in the intelligence areas, but also carry out a risk assessment for each entity subject to its supervision. Other risk criteria could be defined, such as those relating to the future development of intelligence, the organisation of tasks, the complexity of the legal basis or the cross-cutting nature of activities.

Adapt the inspection manual and making reports easier to read

The inspection manual offers considerable leeway in its application. It should be adapted to ensure consistency of approach, better traceability of documentation and better definition of the quality assurance process.

The Head of the Federal Department of Defence, Civil Protection and Sport is the end recipient of the reports. The reports are generally too detailed and therefore relatively long. It is sometimes difficult to keep track of all the findings, assessments and recommendations. The SFAO recommended making the reports easier to read.

Review IT system security

Although it is already aware of the risks associated with its IT infrastructure and information processing, the OA-IA should conduct a critical review of the security documentation for its own systems. In order to fully assess the risks, it should request and consult the IT security documentation developed by its service providers and by the bodies that own the systems used for inspections. The documentation should be adapted and any inconsistencies corrected.

Original text in French

Prise de position générale de l'Autorité de surveillance indépendante des activités de renseignement

> L'AS-Rens remercie le CDF pour sa coopération et ses critiques constructives. Les recommandations du CDF portent principalement sur des thèmes qui figuraient déjà au centre des préoccupations de l'AS-Rens et qui sont en cours d'adaptation ou de développement.
>
> **Texte original en allemand**

1 Mission et déroulement

1.1 Contexte

En 2017, avec l'introduction de la Loi fédérale sur le renseignement (LRens), le Conseil fédéral a créé l'Autorité de surveillance indépendante des activités de renseignement (AS-Rens). Sur proposition du Département fédéral de la défense, de la protection de la population et des sports (DDPS), c'est le Conseil fédéral qui nomme le chef/la cheffe pour une période de six ans.

Son statut est fixé à l'article 77 LRens et dans l'Ordonnance sur la surveillance des activités de renseignement (OSRens). Elle est indépendante. L'Autorité est rattachée administrativement au DDPS (voir extrait en annexe 3). L'AS-Rens dispose de son propre budget d'un peu plus de 2 millions de francs par an, principalement pour couvrir ses dépenses de personnel (9 équivalents temps plein). Son organisation et ses méthodes de travail sont formalisées dans le règlement interne de l'Autorité de surveillance indépendante des activités de renseignement [1]. L'AS-Rens n'est soumise à aucune norme d'audit.

Les tâches de l'AS Rens sont définies à l'article 78 de la LRens. Elle surveille les activités de renseignement du Service de renseignement de la Confédération (SRC), des organes cantonaux d'exécution ainsi que des autres entités et tiers mandatés par le SRC. Son objectif est de contrôler les activités de renseignement quant à leur légalité, leur adéquation et leur efficacité. Un rapport d'activité est publié chaque année. Les résultats des inspections sont communiqués par écrit dans des rapports adressés au DDPS. L'AS-Rens peut formuler des recommandations. Conformément à la LRens, le DDPS veille à la mise en œuvre des recommandations. En cas de rejet, ce dernier doit les soumettre au Conseil fédéral pour décision.

Il s'agit du premier audit que le CDF effectue auprès de l'AS-Rens.

1.2 Objectif et questions d'audit

L'objectif d'audit est de vérifier si l'AS-Rens surveille les activités de renseignement selon l'article 78 LRens. L'application de son règlement et des directives internes qui en découlent fait partie intégrante de cet objectif. Les questions d'audit sont les suivantes :

1. La surveillance exercée par l'AS-Rens sur le domaine du renseignement est-elle conforme aux tâches fixées dans la LRens ?
2. Les ressources en personnel de l'AS-Rens garantissent-elles la surveillance adéquate des domaines d'activités de renseignement, cela auprès de tous les acteurs impliqués ?
3. L'environnement IT, comme outil de travail, permet-il d'effectuer les tâches de surveillance de manière efficace ?

[1] RS 121.31.

1.3 Etendue de l'audit et principe

En application de l'article 8 alinéa 1 lettre a de la Loi sur le Contrôle des finances (LCF), l'AS-Rens, en tant qu'unité décentralisée définie dans l'Ordonnance sur l'organisation du gouvernement et de l'administration (OLOGA), est soumise à la surveillance du CDF.

Le CDF a sélectionné un échantillon de six dossiers d'inspections, trois en 2021 et trois en 2022, répartis dans les six domaines de surveillance définis par l'AS-Rens[2]. Il a procédé à une analyse des documents de travail et effectué des interviews avec les audités et les responsables de ces six inspections.

Le contrôle par échantillon avait pour objectif de vérifier la traçabilité de la documentation et l'application des méthodes de travail durant toutes les phases d'inspection (préparation, exécution et rapport). L'analyse des rapports s'est concentrée sur l'existence d'un fil rouge entre les constatations, les appréciations et les recommandations.

Le CDF n'a pas audité la coordination des activités de l'AS-Rens avec la haute surveillance parlementaire et avec d'autres autorités de surveillance de la Confédération et des cantons selon l'article 78 LRens.

L'audit a été mené du 14 août au 1er septembre 2023 par Alexandre Bläuer (responsable de révision) et Jean-Marc Blanchard (expert en audit). Il a été conduit sous la responsabilité de Prisca Freiburghaus. Le présent rapport ne prend pas en compte les développements ultérieurs à l'audit.

1.4 Documentation et entretiens

Les informations nécessaires ont été fournies au CDF de manière exhaustive et compétente par toutes les personnes impliquées. Les documents (ainsi que l'infrastructure) requis ont été mis à disposition de l'équipe d'audit sans restriction.

1.5 Discussion finale

La discussion finale a eu lieu le 1er novembre 2023. Les participants étaient pour l'AS-Rens, la cheffe, son suppléant et un directeur d'inspection, pour le CDF, le responsable de mandats du DDPS, la responsable de la supervision de l'audit et le team d'audit.

Le CDF remercie l'attitude coopérative et rappelle qu'il appartient à l'AS-Rens de surveiller la mise en œuvre des recommandations.

CONTRÔLE FÉDÉRAL DES FINANCES

[2] Rapport d'activités 2022 de l'AS-Rens, page 6, activités de surveillance : stratégie et planification, organisation, collaboration, recherche, ressources et traitement des données et archivage.

2 Activités de surveillance de l'AS-Rens

2.1 Activités de surveillance en conformité avec la LRens

L'AS-Rens respecte le cadre légal. Elle a défini un règlement interne. Sa structure organisationnelle est directe et plate[3]. Elle dispose de l'indépendance pour s'organiser et définir son mode de fonctionnement, ses processus et ses ressources.

L'appréciation des risques permet de définir les thèmes et établir le plan annuel des inspections. Pour garantir une coordination des activités, un projet est adressé à la haute surveillance parlementaire et aux autorités de surveillance de la Confédération et des cantons.

L'AS-Rens définit des mandats et effectue des inspections auprès des entités soumises à sa surveillance. Le résultat de chaque inspection est formulé dans un rapport. L'AS-Rens émet des recommandations.

Les audités et le Secrétariat général du DDPS estiment que la démarche d'inspection est transparente et le travail professionnel. Ils jugent que les rapports sont de bonne qualité, mais qu'ils pourraient être plus critiques, notamment en formulant des recommandations plus précises.

Sa légitimité en tant qu'autorité de surveillance indépendante n'est pas remise en cause. L'AS-Rens remplit un rôle de prévention et de surveillance reconnu. Les entités soumises à la surveillance de l'AS-Rens recourent aux résultats d'inspection pour accélérer des changements. A titre d'exemple, certaines recommandations permettent de faire évoluer des approches cloisonnées, de renforcer la collaboration et de mieux exploiter les synergies au sein des entités auditées.

Appréciation

La surveillance exercée par l'AS-Rens sur le domaine du renseignement est en adéquation avec la LRens. L'AS-Rens remplit ses tâches de surveillance dans le domaine du renseignement. Elle dispose d'une structure organisationnelle et d'un effectif adaptés à sa mission. En transmettant son projet de plan annuel des inspections, l'AS-Rens apporte sa contribution à une approche coordonnée des activités de surveillance.

L'audit a permis d'identifier des améliorations afin de renforcer l'efficacité de la surveillance. Elles sont décrites aux chapitres 2.2 à 2.4.

2.2 Documentation des risques à développer

Durant l'année, tous les collaborateurs de l'AS-Rens peuvent formuler des idées d'inspection. Elles sont enregistrées dans un dossier centralisé, dénommé « Themenspeicher ». Chaque année, l'AS-Rens organise une retraite de quelques jours avec l'ensemble de ses collaborateurs. Un des objectifs est d'établir le plan annuel des inspections de l'année suivante. Tous les collaborateurs procèdent ainsi collégialement à l'évaluation et la priorisation des thèmes d'inspection.

[3] Une cheffe, huit directeurs d'inspection (dont un est aussi le suppléant de la cheffe) et une responsable de la gestion administrative.

Pour identifier les thèmes d'inspection, l'AS-Rens concentre son analyse de risques sur les six domaines suivants : stratégie et planification, organisation, collaboration, recherche, ressources et traitement des données et archivage. Cependant, elle ne dispose pas de cartographie globale et structurée des risques de tous les domaines du renseignement et de toutes les entités soumises à sa surveillance. Les risques et les défis relatifs au développement futur du domaine du renseignement ne sont pas décrits.

L'AS-Rens est en train de développer un concept d'appréciation des risques pour définir son approche de surveillance des services de renseignement cantonaux (SRcant).

Les mandats sont formulés conformément à la LRens. Selon la loi, traiter les trois thématiques dans chaque mandat – légalité, adéquation, efficacité – n'est pas obligatoire. L'objectif et les questions d'inspection ne sont pas toujours articulés de manière précise.

Appréciation

L'AS-Rens dispose d'une analyse de risques pour définir ses mandats d'inspection. Pour apprécier pleinement les risques liés aux activités de renseignement et suivre leur évolution dans le temps, l'AS-Rens devrait disposer d'une vue globale des risques liés au renseignement. Elle devrait être complétée pour chaque entité soumise à sa surveillance. D'autres critères de risques pourraient être définis, comme ceux relatifs au développement futur du domaine du renseignement (ses défis) ainsi que ceux concernant l'organisation des tâches, la complexité de la base légale ou la transversalité des activités.

Recommandation 1 (Priorité 2)

Le CDF recommande à l'Autorité de surveillance indépendante des activités de renseignement de renforcer son processus d'analyse de risques entre autres par une appréciation globale des risques du domaine du renseignement ainsi que par entité soumise à sa surveillance.

La recommandation est acceptée.

Prise de position de l'Autorité de surveillance indépendante des activités de renseignement

Le processus d'analyse de risques permet à l'AS-Rens de reconnaître les risques qu'elle surveille dans le domaine du renseignement. Le mandat de l'AS-Rens n'est cependant pas celui d'apprécier toute sorte de risques assumés par les entités soumises à sa surveillance.

Ce processus est discuté en permanence en fonction des évolutions dans le domaine. L'AS-Rens tiendra compte de la proposition du CDF la prochaine fois que ce processus sera révisé.

Texte original en allemand

2.3 Renforcer l'unité de doctrine dans l'application des processus d'inspection

L'AS-Rens dispose d'un manuel d'organisation et d'un manuel d'inspection. Ils sont en cours d'actualisation. Le manuel d'inspection couvre toutes les phases d'une inspection et sert de guide aux directeurs d'inspection. Il comporte des erreurs et des incohérences. Le chapitre sur l'assurance qualité est décrit de manière trop succincte.

L'application des processus internes et du manuel d'inspection ne suit pas une unité de doctrine stricte. Les directeurs d'inspection disposent d'une grande marge de manœuvre.

Pour chaque inspection, le manuel prévoit quels documents clés devraient assurer la traçabilité de l'information. Il s'agit notamment du concept d'inspection, du mandat, du résumé des étapes d'inspection (dénommé « Audit Summary ») et du rapport. Sur la base du contrôle des dossiers d'inspection effectué par le CDF, le fil rouge entre les constatations, les appréciations et les recommandations n'est pas toujours garanti. A titre d'exemple, l'« Audit Summary » devrait permettre d'identifier les éléments probants et ainsi faire le lien avec le rapport. Les constatations principales ne sont toutefois pas systématiquement formulées par un texte parlant. Elles renvoient parfois à un protocole d'interview ou à un contrôle par échantillon, pour lesquels aucune conclusion ni résumé n'ont été formulés.

A l'exception des mandats et des rapports, les contrôles liés à l'assurance qualité ne sont pas documentés par un système de visa ou de signature selon le principe des quatre yeux, notamment parce que la liste de contrôle de l'assurance qualité n'est plus utilisée. Ainsi la traçabilité n'est pas garantie. Confirmé lors des entretiens avec les directeurs d'inspection, l'assurance qualité est qualifiée « de partiellement informelle ». Le contrôle des dossiers a montré que l'assurance qualité n'a pas toujours été efficace. Dans un cas par exemple, les documents chiffrés et consultés dans le Réseau informatique sécurisé au SRC n'avaient pas été supprimés. Dans un autre cas, un document confidentiel et interne à l'AS-Rens n'était pas chiffré. Dans plusieurs dossiers d'inspection, tous les documents clés n'étaient pas signés ou cochés conformément au manuel d'inspection.

L'AS-Rens ne planifie pas le nombre de jours par inspection. Le suivi de l'avancement des travaux d'inspection est effectué de manière pragmatique, bimensuellement par la cheffe de l'AS-Rens, lors des séances opérationnelles avec tous les directeurs d'inspection, et dans le cadre des entretiens bilatéraux.

Le suivi des recommandations se fait à l'aide de fichiers Excel tenus séparément par le Secrétariat général du DDPS, par le SRC et par l'AS-Rens. La LRens ne définit toutefois aucun rôle à cette dernière pour assurer un suivi de ses recommandations. Un échange biannuel est organisé par l'AS-Rens pour vérifier leur mise en œuvre. Les risques liés à la mise en œuvre ou non des recommandations sont ainsi considérés dans la formulation des futurs mandats d'inspection et dans l'exécution des inspections en cours.

Appréciation

Le manuel d'inspection devrait être revu et adapté. En complément à la définition des documents clés à produire pour chaque inspection, l'AS-Rens devrait spécifier un contenu minimal obligatoire. Cela permettrait de renforcer l'unité de doctrine, d'assurer une meilleure traçabilité de l'information et de réaliser une assurance qualité plus efficace.

L'assurance qualité devrait être documentée par un système de visa pour toutes les étapes clés d'une inspection. Elle devrait assurer le respect des processus et fixer des exigences plus précises en matière de documentation. Un contrôle par sondage pourrait être introduit.

La comparaison des jours planifiés avec les jours effectivement utilisés permettrait à l'AS-Rens de quantifier les écarts. Cette information serait utile au controlling pour atteindre trois objectifs : améliorer la planification, surveiller et piloter les inspections sous l'angle de l'utilisation des ressources et prendre d'éventuelles mesures pour renforcer la gestion du personnel. Compte tenu de la taille de l'organisation et en raison de la charge administrative correspondante, le CDF renonce à émettre une recommandation sur ce point.

Recommandation 2 (Priorité 2)

Le CDF recommande à l'Autorité de surveillance indépendante des activités de renseignement d'adapter son manuel d'inspection. Ceci afin d'être cohérent avec la définition de la stratégie de surveillance, de garantir une meilleure unité de doctrine dans son application et de renforcer l'assurance qualité.

La recommandation est acceptée.

Prise de position de l'Autorité de surveillance indépendante des activités de renseignement

Une fois par année, l'AS-Rens met à jour son manuel d'inspection. Après cinq ans d'activité, elle a entrepris une révision plus approfondie, durant laquelle elle suivra les recommandations du CDF.

Texte original en allemand

2.4 Renforcer la lisibilité des rapports

Le CDF a procédé à une lecture critique de neuf rapports d'inspection, dont six ont fait l'objet d'un contrôle des dossiers de travail. Les constats principaux sont les suivants :

- Les rapports sont focalisés sur les risques de non-conformité légale et moins sur la non-adéquation ou l'inefficacité des activités de surveillance ;
- La formulation des résumés est insuffisante pour obtenir une appréciation critique. L'objectif de l'AS-Rens est de les utiliser pour la communication externe ;
- Les rapports présentent des descriptions de situation ou de processus détaillés. L'absence de structure par sous-chapitres rend la lecture toutefois difficile ;
- Le fil rouge entre les constatations, les appréciations et les recommandations n'est pas toujours évident à établir. L'AS-Rens inclut systématiquement les constats dans les appréciations ;
- Dans certains cas, les recommandations sont complexes ou pas orientées sur les risques identifiés. Elles sont difficilement compréhensibles hors contexte, sans recourir au rapport, ce qui ne facilite par leur suivi. Leur renvoi à la fin du rapport rend la lecture plus difficile ;
- Le traitement et l'intégration des prises de position dans le rapport n'est pas uniforme ;
- Le nombre de pages des rapports se situe entre 30 et 40.

Appréciation

La compréhension et l'articulation des rapports devraient être améliorées. Même si l'AS-Rens n'est soumise à aucune norme, le fil rouge entre les constatations, les appréciations et les recommandations devrait être mieux garanti.

La structure, le niveau de détail et le nombre de pages élevé des rapports ne permettent pas une lecture efficace pour apprécier tous les objectifs et les résultats d'inspection.

Pour assurer une communication efficace avec le destinataire principal, la cheffe du DDPS, la lisibilité des rapports devrait être améliorée. Les rapports devraient comprendre un résumé succinct avec toutes les informations clés de l'inspection. L'objectif du résumé ne devrait pas se limiter à remplir une fonction de communication externe.

Recommandation 3 (Priorité 2)

Le CDF recommande à l'Autorité de surveillance indépendante des activités de renseignement d'améliorer la lisibilité des rapports, notamment pour renforcer leur impact.

La recommandation est acceptée.

Prise de position de l'Autorité de surveillance indépendante des activités de renseignement

L'AS-Rens s'efforce d'assurer la lisibilité et la vue d'ensemble des conclusions tirées dans ses rapports tout en veillant à les améliorer sans relâche.

Texte original en allemand

3 Les ressources en personnel de l'AS-Rens

Durant ses premières années d'existence, l'AS-Rens a dû acquérir les connaissances nécessaires pour apprécier les activités liées au domaine du renseignement. Suite à une forte rotation de son personnel les deux dernières années, l'AS-Rens a subi une perte de connaissances importante. En septembre 2023, presque tous les postes de directeurs d'inspection étaient repourvus. Les collaborateurs sont motivés et conscients des risques relatifs au traitement et à la confidentialité des informations. La séniorité de plusieurs directeurs d'inspection garantit le transfert de savoir et un niveau de connaissances suffisant pour exécuter les inspections.

L'AS-Rens a développé un programme d'onboarding interne et externe sur trois mois. Il permet d'acquérir à court terme les connaissances sur les règles et les processus internes, mais aussi de se faire une idée générale sur l'organisation des entités soumises à sa surveillance ainsi que sur les domaines d'activités du renseignement. Des séances bilatérales avec la cheffe AS-Rens servent à identifier les besoins et à assurer un suivi durant la période d'essai.

L'AS-Rens dispose d'une cartographie des compétences et des connaissances de chaque collaborateur. Les besoins en formation sont thématisés lors des séances bilatérales entre la cheffe de l'AS-Rens et les directeurs d'inspection, ce qui permet de définir les axes de développement du personnel. L'AS-Rens dispose d'un budget pour la formation.

Selon leur première ou deuxième formation, les directeurs d'inspection sont majoritairement juristes. C'est aussi le cas des trois derniers collaborateurs engagés par l'AS-Rens. Sur les huit personnes occupant cette fonction, deux disposent des qualifications requises dans le domaine de l'audit[4]. Bien que l'AS-Rens ne soit soumise à aucune norme d'audit, le contrôle des papiers de travail des six inspections montre que les techniques d'audit et la traçabilité de l'information présentent un potentiel d'amélioration.

Appréciation

Le niveau de connaissances sur l'activité des entités soumises à la surveillance de l'AS-Rens est essentiel pour que les directeurs d'inspection puissent apprécier les risques, formuler des mandats d'inspection et écrire des rapports et des recommandations pertinentes.

Pour assurer une gestion efficace du savoir et maintenir les directeurs d'inspection expérimentés, il convient d'identifier et de conserver les personnes clés. Face à un environnement complexe qui évolue rapidement, l'AS-Rens doit aussi développer et acquérir les compétences nécessaires rapidement.

Le profil actuel majoritairement juridique des directeurs d'inspection s'aligne sur l'objectif de contrôler les activités du renseignement sous l'angle de la légalité. En revanche, en ce qui concerne l'adéquation et l'efficacité, des compétences et des connaissances plus pointues sont nécessaires. Sans être exhaustif, les aptitudes suivantes sont importantes : la gestion d'entreprise, l'analyse financière, l'évaluation, la sécurité informatique, la digitalisation et l'audit.

[4] Expert-comptable, Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA), Certified Fraud Examiner (CFE).

Pour effectuer ses activités de contrôles, l'AS-Rens doit disposer de compétences variées et étendues dans plusieurs domaines. Un bon équilibre des forces permet aussi de garantir un transfert de savoir. Avec seulement deux directeurs d'inspection formés spécifiquement au métier de l'audit, le savoir est concentré sur un petit nombre de personnes clés. Dans le cadre des futurs recrutements, l'AS-Rens pourrait encore renforcer ses compétences, notamment dans les techniques d'audit, pour mieux surveiller les activités de renseignement sous l'angle de l'adéquation et de l'efficacité.

Comme les outils déployés par l'AS-Rens permettent toutefois d'assurer le développement des compétences et des connaissances des directeurs d'inspection, le CDF ne voit pas la nécessité d'émettre une recommandation.

4 L'infrastructure et les documents de sécurité informatique

4.1 L'environnement informatique est adéquat

L'infrastructure de travail de l'AS-Rens se compose de différents éléments en fonction de la classification des informations à traiter. L'Autorité dispose de l'infrastructure et des accès nécessaires pour remplir ses tâches.

L'audit n'a pas identifié d'inadéquation dans l'utilisation des systèmes informatiques.

L'AS-Rens dispose des instructions liées à l'utilisation des systèmes et au traitement de l'information ainsi que d'une stratégie de formation pour ses collaborateurs[5].

Appréciation

L'environnement informatique permet de garantir une surveillance adéquate des activités de renseignement. Les instructions sont claires et adaptées. Dans le cadre du contrôle par échantillon de six inspections, les directives internes ont été appliquées, à l'exception des éléments signalés au chapitre 2.3.

4.2 Les documents de sécurité informatique sont à améliorer

Durant la phase de préparation (juin 2023), le CDF a communiqué le constat selon lequel les documents principaux en lien avec la sécurité IT existent, notamment une analyse des besoins de protection (dite « Schutzbedarfsanalyse » – SCHUBAN), un concept de mise en œuvre de protection informatique de base et un concept de sûreté de l'information et protection des données (SIPD). Dans le cadre du travail de surveillance de l'AS-Rens, ces documents traitent de manière globale les systèmes utilisés. Ils ne sont pas actualisés et ne sont pas signés par la cheffe de l'AS-Rens. Ils contiennent des informations erronées, contradictoires et pas assez précises.

L'AS-Rens a ensuite pris des mesures de correction qui restent cependant insuffisantes. Sans avoir connaissance des documents de sécurité des systèmes hébergés et gérés par d'autres acteurs ou fournisseurs de prestations, l'AS-Rens ne peut pas apprécier pleinement les risques informatiques liés à son activité de surveillance et ainsi prendre les mesures nécessaires.

En outre, l'appréciation des risques liés à l'utilisation de l'infrastructure pour traiter les informations classées « SECRET » n'est pas suffisante. Les documents de sécurité des systèmes « SCHUBAN » et « Mise en œuvre des mesures de protection informatique de base » ne sont pas développés spécifiquement pour l'objet à protéger. Ces deux documents comportent encore des erreurs, notamment l'appréciation du risque lié au traitement des données personnelles. La « Mise en œuvre des mesures de protection informatique de base » a été écrite pour l'objet de protection géré par l'OFIT, alors qu'il devrait l'être pour l'infrastructure utilisée pour traiter les informations classées « SECRET ». Le concept « Information Security Management System » est mal nommé, il s'agit bien plus d'un concept SIPD.

[5] Manuel d'organisation de l'AS-Rens du 1er octobre 2021.

Appréciation

L'AS-Rens effectue ses activités d'inspection dans un milieu sensible au traitement de l'information. Cela expose sa réputation et sa crédibilité, mais aussi peut mettre en péril la vie d'être humain.

La perte ou le vol d'informations et l'utilisation illégale des outils informatiques sont des risques inhérents à réduire, notamment par la formation et la sensibilisation des directeurs d'inspection, mais aussi par une appréciation précise des risques des objets à protéger. Par conséquent, l'AS-Rens devrait obtenir les documents de sécurité informatique de ses fournisseurs de prestations et des propriétaires d'objets à protéger.

L'analyse de risques des objets à protéger devraient être renforcée. Les documents de sécurité informatique devraient être améliorés et les incohérences corrigées.

Recommandation 4 (Priorité 2)

Le CDF recommande à l'Autorité de surveillance indépendante des activités de renseignement d'effectuer une revue critique des documents de sécurité des systèmes informatiques. La qualité des documents « SCHUBAN », « Mise en œuvre des mesures de protection informatique de base » et « Concept SIPD » devrait être améliorée.

La recommandation est acceptée.

Prise de position de l'Autorité de surveillance indépendante des activités de renseignement

Ayant déjà pu consulter la documentation du SRC, l'AS-Rens s'en inspirera pour la révision des documents de ses propres systèmes. Une demande de consultation du document de de sécurité de l'information et protection des données (SIPD) de l'environnement de l'OFIT a déjà été déposée auprès du SG-DDPS, mais la réponse se fait attendre.

Texte original en allemand

Annexe 1 : Bases légales

Textes législatifs
Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) du 21 mars 1997, RS 120
Loi fédérale sur le renseignement (LRens) du 25 septembre 2015, RS 121
Ordonnance sur le service de renseignement (Ordonnance sur le renseignement, ORens) du 16 août 2017, RS 121.1
Ordonnance sur les systèmes d'information et des systèmes de stockage de données du Service de renseignement de la Confédération (OSIS-SRC) du 16 août 2017, RS 121.2
Ordonnance sur la surveillance des activités de renseignement (OSRens) du 16 août 2017, RS 121.3
Ordonnance sur l'organisation du gouvernement et de l'administration (OLOGA) du 25 novembre 1998, RS 172.010.1
Loi sur l'Assemblée fédérale (Loi sur le Parlement, LParl) du 13 décembre 2002, RS 171.10
Loi fédérale sur l'armée et l'administration militaire (Loi sur l'armée, LAAM) du 3 février 1995, RS 510.10
Ordonnance concernant le Service de renseignement de l'armée (OSRA) du 4 décembre 2009, RS 510.291
Loi fédérale sur le Contrôle fédéral des finances (Loi sur le Contrôle des finances, LCF) du 28 juin 1967, RS 614.0
Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 18 mars 2016, RS 780.1
Règlement
Règlement interne de l'autorité de surveillance indépendante des activités de renseignement du 26 février 2018

Annexe 2 : Abréviations

AS-Rens	Autorité de surveillance indépendante des activités de renseignement
CDF	Contrôle fédéral des finances
CFE	Certified Fraud Examiner
CIA	Certified Internal Auditor
CISA	Certified Information Systems Auditor
DDPS	Département fédéral de la défense, de la protection de la population et des sports
ISDS	Informationssicherheit und Datenschutz
LCF	Loi fédérale sur le Contrôle fédéral des finances
LRens	Loi fédérale sur le renseignement
OFIT	Office fédéral de l'informatique et de la télécommunication
RM	Renseignement militaire
SCHUBAN	Schutzbedarfsanalyse
SIPD	Sûreté de l'information et protection des données
SRA	Service de renseignement de l'armée
SRC	Service de renseignement de la Confédération
SRCant	Service de renseignement cantonal

Annexe 3 : Extrait de la loi fédérale sur le renseignement, articles 75 à 78

Section 2 Contrôle et surveillance du SRC

Art. 75 Auto-contrôle du SRC

Le SRC s'assure par des mesures de contrôle appropriées, qui porteront notamment sur la qualité, de la bonne exécution de la présente loi, tant en son sein que par les autorités cantonales compétentes en matière de sécurité.

Art. 76 Autorité de surveillance indépendante

1 Le Conseil fédéral crée une autorité de surveillance indépendante chargée de la surveillance du SRC.

2 Il en nomme le chef sur proposition du DDPS pour une période de fonction de six ans.

3 Le chef de l'autorité de surveillance indépendante est nommé tacitement pour chaque nouvelle période de fonction, à moins que le Conseil fédéral décide de ne pas renouveler celle-ci pour des motifs objectifs suffisants au plus tard six mois avant son échéance.

4 Il peut demander au Conseil fédéral, en respectant un délai de six mois, de mettre fin à la période de fonction pour la fin d'un mois.

5 Le Conseil fédéral peut révoquer le chef de l'autorité de surveillance indépendante avant la fin de sa période de fonction :

a. s'il a violé gravement ses devoirs de fonction de manière intentionnelle ou par négligence grave ;

b. s'il a durablement perdu la capacité d'exercer sa fonction.

Art. 77 Statut de l'autorité de surveillance indépendante

1 L'autorité de surveillance indépendante exerce ses fonctions de manière indépendante et sans être liée par des instructions. Elle est rattachée administrativement au DDPS.

2 Elle dispose de son propre budget. Elle engage son personnel.

3 Elle se constitue elle-même. Elle fixe son organisation et ses méthodes de travail dans un règlement.

4 Les rapports de travail du chef de l'autorité de surveillance indépendante et du personnel sont régis par la loi du 24 mars 2000 sur le personnel de la Confédération. Le chef de l'autorité de surveillance indépendante n'est pas soumis au système d'évaluation prévu à l'art. 4, al. 3, de ladite loi.

Art. 78 Tâches, droit à l'information et recommandations de l'autorité de surveillance indépendante

1 L'autorité de surveillance indépendante surveille les activités de renseignement du SRC, des organes cantonaux d'exécution ainsi que des autres entités et des tiers mandatés par le SRC. Elle contrôle ces activités quant à leur légalité, leur adéquation et leur efficacité.

2 Elle coordonne ses activités avec la haute surveillance parlementaire et avec d'autres autorités de surveillance de la Confédération et des cantons.

3 Elle informe le DDPS de ses activités dans un rapport annuel à publier.

4 Elle a accès à toutes les informations et à tous les documents utiles ainsi qu'à tous les locaux utilisés par les entités soumises à la surveillance. Elle peut exiger des copies des documents consultés. Dans le cadre de l'accomplissement de ses tâches de surveillance, elle peut demander à d'autres services de la Confédération et des cantons de lui fournir des informations et de la laisser prendre connaissance des dossiers, dans la mesure où ces informations ont un lien avec la collaboration entre ces services et les entités soumises à la surveillance.

5 Pour accomplir ses tâches, l'autorité de surveillance indépendante peut accéder à tous les systèmes d'information et à tous les fichiers des entités soumises à la surveillance ; elle peut également accéder en ligne aux données sensibles. Elle ne peut conserver les données dont elle a ainsi eu connaissance que jusqu'à l'aboutissement de la procédure de contrôle. Les accès aux différents fichiers doivent être consignés dans un journal par le maître du fichier.

6 L'autorité de surveillance indépendante communique le résultat de ses contrôles par écrit au DDPS. Elle peut form[ul]er des recommandations.

7 Le DDPS veille à la mise en œuvre de ces recommandations. Si le DDPS rejette une recommandation, il la soumet au Conseil fédéral pour décision.

Annexe 4 : Echantillon des six dossiers d'inspections de l'AS-Rens audités par le CDF

Inspection	Numéro	Domaine	Année	Audité
Service de renseignement cantonal Vaud (SRCant VD)	21-11	Collaboration	2021	SR cantonal VD et SRC
Operationen	21-14	Recherche d'informations	2021	SRC
Datenschutz im Militärischen Nachrichtendienst	21-18	Traitement des données, archivages	2021	SRM
Früherkennung und Antizipation	22-01	Stratégie et planification	2022	SRC
Beschaffungsmanagement	22-11	Recherche d'informations	2022	SRC
Follow-up 20-19 : les archives du SRC	22-17	Traitement des données, archivages	2022	SRC

Priorités des recommandations

Le Contrôle fédéral des finances priorise ses recommandations sur la base de risques définis (1 = élevés, 2 = moyens, 3 = faibles). Comme risques, on peut citer par exemple les cas de projets non-rentables, d'infractions contre la légalité ou la régularité, de responsabilité et de dommages de réputation. Les effets et la probabilité de survenance sont ainsi considérés. Cette appréciation se fonde sur les objets d'audit spécifiques (relatif) et non sur l'importance pour l'ensemble de l'administration fédérale (absolu).