Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Sozialversicherung BSV
Direktionstab DS – IT Management ITM

Communication eGov n° 058 de 04.06.2025

A adresser à : Organes d'exécution du 1er pilier/AFam

Concerne : Audits informatiques selon DASP et D-SIPD

Suite au projet «Modernisation de la surveillance du 1er pilier[1]», les organes d'exécution du 1er pilier/AFam doivent disposer d'un système de gestion de la sécurité de l'information (SGSI).

La mise en œuvre du SGSI est contrôlée chaque année par les organes de révision des organes d'exécution du 1er pilier/AFam.

Situation initiale et principe

Avec la modification de la loi fédérale sur l'assurance-vieillesse et survivants, la modernisation de la surveillance du 1er pilier et l'optimisation du 2e pilier de la prévoyance vieillesse, survivants et invalidité, l'OFAS charge les organes d'exécution de veiller à ce que leurs systèmes d'information tiennent compte en permanence des nouvelles conditions-cadres décrites ci-après.

L'un des objectifs centraux de la révision de la loi est que les systèmes d'information du 1er pilier disposent de la stabilité et de la capacité d'adaptation nécessaires et garantissent la sécurité des informations et la protection des données.

Pour cette raison, les organismes d'exécution du 1er pilier/AFam sont tenus de faire réaliser des audits informatiques annuels par des auditeurs informatiques certifiés à partir du 1er janvier 2025. Les audits informatiques sont effectués conformément à l'art. 159, let. c, RAVS et à l'art. 160, al. 5, RAVS par les organes de révision, la participation de sous-traitants étant autorisée.

Il convient ici de rappeler que l'OFAS a déjà informé avec la communication eGov 043 du 1.1.22 que les recommandations dans le domaine de la sécurité de l'information et de la protection des données, publiées depuis 1.1.2022, seront la base pour les directives qui entreraient en vigueur avec le projet de loi pour la modernisation de la surveillance (entrée en vigueur le 1.1.2024). L'OFAS a plusieurs fois échangé à ce sujet avec les présidences des conférences au sein du comité de pilotage 1er pilier/AFam (voir le procès-verbal de la séance du 4.7.2022 et la réponse de l'OFAS à la lettre des conférences à ce sujet ainsi que le procès-verbal de ls séance du 12.2.2024). L'OFAS a également échangé et informé les délégués des conférences au sein de la commission de coordination eGov (CoCo eGov) à ce sujet et précisé que l'introduction des directives D-SIPD (exigences SIPD) se fera à partir du 1.1. 2024 et a repoussé au 1.1.2025 l'introduction des audits IT selon les directives DASP suite à la demande des délégués des conférences de la CoCo eGov (voir procès-verbal de la CoCo eGov du 4.12.2023 qui intègre la recommandation des délégués des conférences de la CoCo eGov pour la validation des directives S-SIPD et des directives DASP). Plusieurs autres séances de la CoCo eGov ont également traité le sujet depuis 2020 (voir exemple avec le procès-verbal de la

[1] Modernisation de la surveillance du 1er pilier: https://www.bsv.admin.ch/bsv/fr/home/assurances-sociales/ueberblick/reformen-revisionen/modernisierung_aufsicht.html

séance du 22.10.2020).

Le cadre et l'étendue des audits informatiques sont définis dans les directives DASP[2] et D-SIPD[3].

La directive D-SIPD contient des instructions relatives aux **exigences en** matière de sécurité de l'information et de protection des données applicables aux systèmes d'information des organes d'exécution du 1er pilier/AFam.

La DASP documente les directives relatives aux audits sur la sécurité de l'information et la protection des données et contient un questionnaire pour les audits informatiques, respectivement les mesures de contrôle requises.

Le secteur ITM

Pour toute autre question, veuillez vous adresser à egov@bsv.admin.ch

[2] DASP: https://sozialversicherungen.admin.ch/fr/d/20260/download
[3] D-SIPD: https://sozialversicherungen.admin.ch/fr/d/20253/download