Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur
Office fédéral des assurances sociales OFAS

Directives concernant les audits sur la sécurité de l'information et la protection des données (DASP)

Valable à partir du 1er janvier 2024

État au 20 Avril 2026

Remarque
Afin de faciliter la lecture, seule la forme masculine est utilisée dans ce document. Il va de soi qu'elle englobe les personnes de tous les genres.

f DASP (318.108.09)

01.24

Avant-propos

Les systèmes d'information du 1er pilier doivent être stables et adaptables tout en garantissant la sécurité de l'information et la protection des données. En s'appuyant sur les directives de l'OFAS, l'organe de révision vérifie que les organes d'exécution remplissent les exigences fixées par l'autorité de surveillance (art. 68*a*, al. 2, let. c, LAVS ; art. 159, let. c, et 160, al. 5, RAVS).

Le chapitre 1 couvre les exigences applicables aux compétences et à la formation des auditeurs informatiques.

Le chapitre 2 couvre les exigences applicables au processus de contrôle de l'audit informatique prévu à l'art. 68*a*, al. 2, let. c, LAVS. La mise en œuvre de ces exigences nécessitera un processus d'adaptation continu, raison pour laquelle un modèle de maturité est introduit et devra être pris en compte par les auditeurs lors de leurs contrôles.

Table des matières

Abréviations

AVS	Assurance-vieillesse et survivants
AC	Assurance-chômage
CdC	Centrale de compensation
ch.	Chiffre
CISA	Certified Information Systems Auditor de l'ISACA
CISM	Certified Information Security Manager de l'ISACA
CISSP	Certified Information Systems Security Professional
ISACA	Information Systems Audit and Control Association
ISC	International Information Systems Security Certification Consortium
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants
OFAS	Office fédéral des assurances sociales
PSI	Préposé à la sécurité de l'information
RAVS	Règlement sur l'assurance-vieillesse et survivants
SGSI	Système de gestion de la sécurité de l'information
TÜV	Technischer Überwachungsverein

Chapitre 1 : Exigences applicables aux responsables des audits informatiques

1.1 Connaissances pratiques

1 Lors de leurs contrôles, les réviseurs établissent si les organes d'exécution remplissent les exigences visées à l'art. 72a, al. 2, let. b, LAVS. Les auditeurs possèdent des connaissances pratiques dans les domaines suivants, ce qui leur donne les compétences nécessaires :

- sécurité de l'information ;
- protection des données ;
- audit informatique.

1.2 Formation et compétences

2 En matière de formation et de compétences, les exigences suivantes doivent être remplies par les responsables des audits informatiques :

- diplôme d'une haute école, d'une haute école spécialisée ou d'une école supérieure, d'une durée d'au moins un an, axée sur la sécurité de l'information et la protection des données, ou
- expérience d'au moins deux ans dans le domaine de la sécurité de l'information ou de l'audit informatique en tant que membre d'une équipe d'audit dans une société de révision agréée. Cette expérience peut également être attestée par des certifications professionnelles reconnues telles que :
  - CISA de l'ISACA ou Lead Auditor de TÜV, ou
  - CISM de l'ISACA ou CISSP de l'ISC.

1.3 Exigences personnelles

3 Les responsables des audits informatiques n'ont ni relation personnelle ni conflit d'intérêts avec l'entité auditée. Ils sont indépendants et impartiaux.

1.4 Contrôle de sécurité relatif aux personnes

4

Le réviseur responsable visé à l'art. 68, al. 2, LAVS s'assure que le responsable de l'audit informatique jouit d'une réputation irréprochable conformément à l'art. 5, al. 1, let. a, de la loi sur la surveillance de la révision (LSR).

1.5 Principes

5 Les responsables de l'audits informatiques se conforment aux principes suivants :

- Comportement éthique : les responsables de l'audit informatique respectent la confidentialité des informations et des renseignements.
- Présentation factuelle : les responsables de l'audit informatique rendent compte fidèlement des résultats de leurs vérifications et présentent les faits de manière compréhensible. Les résultats de l'audit doivent être reproductibles (pour une situation identique).
- Diligence raisonnable : les responsables de l'audit informatique font preuve de diligence lors de l'audit. Leur capacité de discernement est une condition indispensable à la réalisation d'audits pertinents et bien fondés.
- Preuves : les rapports d'audit sont vérifiables. Les résultats peuvent s'appuyer sur un échantillonnage des informations disponibles, car un audit est réalisé sur une période limitée. Cet échantillonnage est pertinent et réalisé à une échelle raisonnable.

Chapitre 2 : Exigences applicables aux audits informatiques

2.1 Principes

6 L’audit informatique est réalisé conformément aux principes suivants :

- Le contenu de l’audit est fondé sur des contrôles informatiques généraux et conforme à la série de normes ISO 27000 reconnues et établies à l’échelle internationale.
- L’audit informatique est réalisé en se fondant sur les risques.
- Les audits annuels couvrent l’ensemble de la période écoulée depuis le dernier audit. En l’absence d’audit précédent servant de référence, l’évaluation porte sur la situation au moment de l’audit actuel.
- L'OFAS peut définir des priorités d'audit.
- Le responsable de l’audit informatique peut en outre fixer d’autres priorités à sa discrétion lors de l’audit informatique.

2.2 Entités auditées

7 Un audit informatique est réalisé auprès des entités suivantes :

- les organes d’exécution, dans la mesure où ils n’ont pas été certifiés conformément à la norme ISO 27001 ou ne sont pas en mesure de produire un rapport d’audit ISAE 3000 de type 1 ou de type 2. Les organes d’exécution certifiés présentent leur rapport de certification ou d’audit à l’organe de révision ;
- les caisses d’allocations familiales, dans la mesure où les caisses de compensation versent des allocations familiales en tant que tâche déléguée ;
- Lorsque plusieurs caisses de compensation, conduites par la même direction, utilisent exactement les mêmes systèmes d’information, un audit unique est suffisant. Le rapport d’audit doit couvrir l’ensemble des caisses de compensation concernées et les mentionner explicitement.

  Les tiers qui fournissent des prestations informatiques pour le compte d’un organe d’exécution audité, qui ont potentiellement accès à des données relevant des assurances sociales ou qui en assurent le traitement (conformément au ch. 2.15 D-SIPD), à moins qu’ils ne soient certifiés ISO 27001, qu’ils disposent d’un

rapport d'audit ISAE 3000 de type 1 ou de type 2, ou d'un rapport d'audit valide conformément au chiffre marginal 14 DASP. Un tel rapport d'audit peut être reconnu comme preuve valable par tous les organes d'exécution qui utilisent les prestations de ce tiers ainsi que par leurs organes de révision, pour autant qu'il ait été établi conformément aux directives DASP et par un organisme d'audit répondant aux exigences définies dans les DASP. Une certification ISO/IEC 27001 existante n'exclut pas que l'auditeur, dans le cadre de son pouvoir d'appréciation, effectue des procédures d'audit supplémentaires auprès de tiers si cela s'avère nécessaire pour l'évaluation finale des contrôles ou de situations pertinentes.

- Il est recommandé aux partenaires contractuels qui disposent d'un rapport d'audit valable, d'une certification ISO 27001 en vigueur ou d'un rapport de vérification ISAE 3000 valable, de les transmettre à l'ensemble des organes d'exécution qui sont clients du partenaire concerné.

2.3 Responsabilités

8 La direction de l'organe d'exécution est responsable du respect des exigences des directives D-SIPD. Elle veille à ce que le responsable de l'audit informatique puisse remplir sa mission, met les informations nécessaires à sa disposition et est son interlocuteur principal.

9 Le préposé à la sécurité de l'information de l'organe d'exécution reste à la disposition de l'OFAS et du responsable de l'audit informatique.

10 L'organe de révision est responsable de la réalisation de l'audit informatique et peut confier le mandat correspondant aussi bien en interne qu'à des tiers externes. En accord avec l'organe de révision, l'audit informatique peut également être mandaté par l'organe d'exécution. L'organe de révision en demeure toutefois responsable. Le responsable de l'audit informatique est chargé du respect des exigences.

2.4 Étendue et déroulement de l'audit

11 L'audit des systèmes d'information permet de contrôler la disponibilité du SGSI conformément aux directives D-SIPD.

12 L'audit comprend les étapes suivantes :

- Vérification des mesures prises en réponse au dernier audit ;
- Vérification de l'efficacité des mesures définies par le préposé à la sécurité de l'information dans le cadre du SGSI ;
- Traitement du questionnaire d'audit informatique standardisé par l'OFAS (cf. annexe 1) ;
- Rédaction d'un rapport d'audit informatique (voir ch. 14 ss) ;
- Examen du rapport d'audit informatique par le préposé à la sécurité de l'information de l'entité auditée et prise de position par celui-ci sur les lacunes constatées par le responsable de l'audit informatique et les mesures proposées ;
- Intégration de la prise de position du préposé à la sécurité de l'information dans le rapport d'audit informatique définitif ;
- Envoi simultané du rapport d'audit informatique par le réviseur responsable, dans un délai d'un mois après la fin de l'audit, au canton ou aux associations fondatrices, au comité de la caisse, à l'OFAS, à la CdC et à l'organe d'exécution audité.

2.5 Rapports

13 Les rapports d'audit informatique doivent être rédigés de façon concise, claire et critique. Ils contiennent toutes les constatations importantes pour les organes d'exécution et les autorités de surveillance. Il convient à ce propos de relever les particularités de chaque organe d'exécution et d'en tenir compte.

14 Le contenu du rapport comprend au moins :

- Indication de la version ;
- Aperçu/synthèse ;
- Résultat de l'audit informatique :

1. Résumé, avec informations sur l’entité auditée et les destinataires ;
2. Aperçu des conclusions de l’audit informatique précédent et de l’état de la mise en œuvre des mesures proposées ;
3. Présentation de l’environnement informatique contrôlé et des contrôles effectués ; présentation des actions de contrôle et de l’étendue de l’audit ;
4. Résultats détaillés des points contrôlés pour chaque chapitre principal des directives D-SIPD ;
5. Résultats de l’examen approfondi ;
6. Appréciation globale ;
7. Propositions d’amélioration ;
8. Confirmation par le réviseur que les responsables des audits informatiques remplissent les exigences prévues aux cm. 2 et 3 ;
9. Confirmation par les auditeurs informatiques dans le rapport d’audit qu’ils sont indépendants, qu’ils n'ont pas de conflits d’intérêts ou de relations personnelles avec l’entité auditée et que les résultats du rapport d’audit reposent sur leurs propres vérifications.
10. Le questionnaire IT auquel il a été répondu, conformément à l'annexe 1.

Lorsqu’un certificat ISO 27001 ou un rapport d’audit ISAE 3000 de type 1 ou de type 2 est soumis, l’organe de révision vérifie les points suivants :

- **ISO 27001 :**
  - Le champ d’application du SGSI certifié englobe toutes les unités organisationnelles et tous les processus d’affaires pertinents des organes d’exécution.
  - La déclaration d’applicabilité du SGSI n’exclut aucune des mesures de sécurité exigées par les directives D-SIPD.
  - Lors de l’audit de (re)certification, toutes les mesures de sécurité exigées par les directives D-SIPD ont été vérifiées.

- **ISAE 3000 de type 1 :**
  - Le rapport d’audit se base sur toutes les conditions fixées dans les directives D-SIPD.

- **ISAE 3000 de type 2 :**
  - Le rapport d’audit est établi avec une certitude suffisante, contrôlé dans le temps et vérifié selon les contrôles définis par les directives D-SIPD.

2.6 Modèle de maturité

15 L'évaluation des résultats se fonde sur le questionnaire d'audit informatique. Le degré de conformité est défini comme suit au moyen du niveau de maturité de l'organisation de la sécurité informatique de l'entité auditée :

Degré de réalisation	Écart	Description	Niveau de maturité
Rempli	Aucune	Les mesures existantes permettent de remplir pleinement les exigences de l'OFAS examinées au moyen des contrôles correspondants.	4
Rempli avec des remarques	Aucune	Les mesures existantes permettent de remplir pleinement les exigences de l'OFAS examinées au moyen des contrôles correspondants. Une remarque est néanmoins formulée.	3
Partiellement rempli	Observations	Les mesures existantes permettent de remplir partiellement les exigences de l'OFAS examinées au moyen des contrôles correspondants.	2
Non rempli	Observations	Les exigences de l'OFAS examinées au moyen des contrôles correspondants ne sont pas remplies.	1

Lorsqu'il existe un soupçon fondé qu'un organe d'exécution ne remplit pas ses obligations en matière de mise en œuvre des exigences relatives à la sécurité de l'information et à la protection des données conformément aux chiffres marginaux 2.1 à 2.18 des D-SIPD (niveau de maturité 1), l'OFAS peut, sur la base de l'art. 72b LAVS, ordonner des mesures de surveillance appropriées. Celles-ci comprennent notamment l'exécution d'un audit extraordinaire aux frais de l'organe d'exécution, l'exigence de justificatifs supplémentaires ou la prescription de mesures assorties d'un délai.

Chapitre 3 : Entrée en vigueur

16 Les présentes directives entrent en vigueur le 1er janvier 2024.

Les premiers audits informatiques seront réalisés à partir du 1er janvier 2025.

Annexe 1 : questionnaire pour les audits informatiques

1 Activités de contrôle

Action de contrôle	Commentaire
Analyse de la documentation	L'exigence des directives D-SIPD est vérifiée au moyen d'une analyse de la documentation existante. Une distinction est faite entre la documentation souhaitée et la documentation réelle. **Documentation de l'objectif** Prescriptions, directives, concepts Plans, instructions d'action, etc. **Documentation sur la situation actuelle** Preuves de la mise en œuvre de la documentation souhaitée. Exportations de données, enregistrements (logs), protocoles, captures d'écran
Vérification du système	Les exigences D-SIPD sont vérifiées directement sur le système d'information concerné. Une vérification sur le système devrait être effectuée via un accès par la personne compétente/responsable concernée sous la supervision de l'auditeur. Des captures d'écran peuvent par exemple être réalisées à titre de preuve.

2 Questionnaire audit informatique

Référence Réf. D-SIPD	Référence ISO 27001:2022	Questionnement	Acte de contrôle requis
2 Exigences			
2.1 Système de gestion de la sécurité de l'information (SGSI)	4.4	L'organe d'exécution a-t-il mis en place et utilise-t-il un SGSI ?	Analyse de la documentation
2.2 Structure du SGSI			
a) Définition des thèmes et des activités liés à la sécurité	4.1	Les thèmes et activités de l'OE liés à la sécurité ont-ils été identifiés et documentés ?	Analyse de la documentation
b) Identification des services impliqués	4.2	Les services impliqués dans la sécurité de l'information de l'OE ont-ils été identifiés, documentés ?	Analyse de la documentation
c) Inventaire des systèmes d'information et des activités liées à l'informatique	A.5.9	Un inventaire des systèmes d'information et des activités liées à l'informatique est-il tenu ? L'inventaire des systèmes d'information est-il mis à jour régulièrement, c'est-à-dire au moins une fois par an ? Existe-t-il un processus pour l'ajout/la suppression de systèmes et d'activités informatiques dans l'inventaire des systèmes d'information ?	Analyse de la documentation
d) Le champ d'application du SGSI est défini	4.3	Les domaines de l'OE qui sont couverts par le SGSI ont-ils été définis et documentés ?	Analyse de la documentation

		Les éventuels domaines ne relevant pas du champ d'application du SGSI sont-ils mentionnés et, dans la négative, l'ensemble de l'organisation est-il indiqué comme champ d'application ?	
e) Le SGSI et ses composantes sont régulièrement mis à jour	4.4	Existe-t-il des actions visibles de mise à jour et d'amélioration continues du SGSI ? [N.B. : généralement, un SGSI contient une liste des opportunités d'amélioration, ce qui permet de documenter l'amélioration continue et d'en assurer la traçabilité]. Existe-t-il des actions visibles pour vérifier chaque année l'actualité du SGSI ?	Analyse de la documentation
2.3 Politique de sécurité de l'information	A.5.1 A.5.3 A.5.5 A.5.24	Des lignes directrices en matière de sécurité de l'information ont-elles été édictées et communiquées aux collaborateurs et aux tiers mandatés, qui contiennent les points énumérés ?	Analyse de la documentation
2.4 Exigences relatives à l'organisation de la sécurité de l'information	A.5.2	Existe-t-il un organigramme de l'organisation de la sécurité de l'information et a-t-il été communiqué ? Les personnes désignées dans l'organigramme savent-elles quelles tâches elles doivent accomplir et quelles sont leurs responsabilités ? L'OE a-t-il défini au moins un rôle central pour la sécurité de l'information (par	Analyse de la documentation

		ex. PSI, CISO ou équivalent) ainsi que d'autres rôles pertinents, et ces rôles ont-ils été documentés ? Les tâches du rôle central ainsi que celles des autres personnes assurant des fonctions clés dans la mise en œuvre de la sécurité de l'information sont-elles documentées de manière contraignante (p. ex. dans un cahier des charges ou une description de poste) ?	
2.5 Exigences relatives aux projets de systèmes d'information	A.5.8	Existe-t-il une méthode de gestion de projet informatique définie qui correspond aux points exigés ? Peut-on identifier des projets informatiques dans lesquels la méthode de gestion de projet a été appliquée ?	Analyse de la documentation
2.6 Sécurité de l'information pour les appareils mobiles et le travail mobile	A.6.7 A.8.1	Une politique sur le travail mobile et les appareils mobiles / BYOD a-t-elle été élaborée et communiquée ? Cette directive contient-elle les éléments requis par les instructions ?	Analyse de la documentation
2.7 Sécurité de l'information et personnel			
2.7.1 Sécurité du personnel	A.6.1 – A.6.5	Existe-t-il des directives sur les obligations en matière d'information, de confidentialité et de systèmes informatiques ? Celles-ci sont-elles com-	Analyse de la documentation

		muniquées aux tiers mandatés et au personnel de l'entreprise ? Existe-t-il un processus de restitution des informations et des moyens informatiques après la fin du contrat de travail du personnel ou du contrat de mandat des tiers mandatés ? Un contrôle de sécurité approprié est-il effectué et mis à jour périodiquement (au moins une fois par an) pour les employés ayant accès à des informations critiques ou ayant des accès privilégiés aux systèmes informatiques ? Le PSI et d'autres rôles clés de l'organisation de la sécurité sont-ils spécifiquement contrôlés au moyen d'un contrôle de sécurité relatif aux personnes ? Le contrôle de sécurité relatif au rôle PSI et d'autres rôles clés inclut-il une vérification du casier judiciaire et du registre des poursuites ?	
2.7.2 Information et formation	A.5.4 A.6.3 A.6.4	Des formations et des sensibilisations des collaborateurs sont-elles organisées au moins une fois par an ? Existe-t-il un concept pour la formation et la sensibilisation des collaborateurs ?	Analyse de la documentation

		Les collaborateurs ont-ils connaissance des obligations et des directives qui leur sont applicables en matière de sécurité de l'information ?	
2.7.3 Changement de situation	A.6.5	Existe-t-il un processus défini pour l'adaptation systématique des droits d'accès et des autorisations d'accès en cas d'adaptation du rapport d'engagement ou de mandat ou de l'accord d'utilisation ? Existe-t-il un processus défini pour traiter les comptes non utilisés et est-il suivi ?	Analyse de la documentation
2.8 Objets de protection des SI : Inventaire, documentation SIPD etautres exigences			
2.8.1 Inventaire des actifs	A.5.9	Tous les systèmes d'information de l'OE font-ils l'objet d'un inventaire et cet inventaire est-il toujours tenu à jour ?	Analyse de la documentation
2.8.2 Documentation de base SIPD	A.5.10 A.5.12 A.5.13	Existe-t-il une documentation SIPD pour les projets et les systèmes d'information et est-elle conforme, qualitativement et quantitativement, au modèle donné dans l'annexe 4 de la D-SIPD ? Ces documentations de base contiennent-elles les éléments requis par système d'information dans les D-SIPD au point 2.8.2, point 2 ?	Analyse de la documentation

2.8.3 Documentation ISDS étendue	A.5.10 A.5.12 A.5.13	Des documentations SIPD étendues contenant les thèmes définis dans les D-SIPD au cm 2.8.3 ont-elles été établies pour les systèmes informatiques avec lesquels des données personnelles sensibles sont traitées ?	Analyse de la documentation
2.8.4 Actualité de la documentation de l'ISDS	-	La documentation SIPD des systèmes d'information exploités correspond-elle à la situation actuelle ?	Analyse de la documentation
2.8.5 Responsable de l'application	A.5.9	Une personne responsable a-t-elle été désignée dans l'inventaire des biens pour chaque objet protégé ? Ces personnes ont-elles connaissance de leurs responsabilités ?	Analyse de la documentation
2.9 Contrôle de l'accès aux systèmes d'information	A.5.15 – A.5.18 A.8.2 – A.8.5	Existe-t-il un concept de contrôle d'accès documenté qui contient au moins les points énumérés dans les D-SIPD Cm 2.9 ? Tous les accès (y c. les processus automatisés avec accès machine-to-machine) aux systèmes d'information sont-ils protégés par une authentification correspondant au besoin de protection et, si nécessaire, par des mesures cryptographiques adéquates conformément à la matrice d'accès définie ?	Analyse de la documentation Vérification du système

		Le principe du « least privilege » est-il appliqué pour les accès ? Les accès aux données personnelles sensibles sont-ils consignés conformément à l'art. 4 OLPD ? L'exactitude et la pertinence des accès sont-elles vérifiées au moins une fois par an ?	
2.10 Cryptographie			
2.10.1 Méthodes et procédures cryptographiques	A.8.24	Les procédés et méthodes cryptographiques utilisés sont-ils conformes aux règles reconnues de la technique ? En cas d'utilisation de certificats-clés, ceux-ci sont-ils délivrés par une autorité de certification (CA) reconnue, en fonction de l'application et des exigences légales qui y sont liées ? Les clés cryptographiques sont-elles gérées de manière sécurisée et leur validité est-elle garantie ?	Analyse de la documentation Vérification du système
2.11 Protection physique			
2.11.1 Dispositif de sécurité pour les locaux	A.7.1 – A.7.3 A.7.5	Les systèmes d'information sont-ils protégés par des mesures de protection physique adéquates en fonction du groupe de protection qui leur est attribué ? • Périmètres de sécurité physique (situation de	Analyse de la documentation

		l'environnement et mesures de construction) • Contrôle d'accès physique • Sécuriser les bureaux, les locaux et les installations • Protection contre les menaces externes et environnementales	
2.11.2 Mesures pour les appareils et les moyens d'exploitation	A.7.7 – A.7.14 A.8.1	Les mesures suivantes de protection des appareils et des moyens d'exploitation sont-elles mises en œuvre de manière appropriée ? • Placement et protection des appareils et des équipements • Services publics • Sécurité du câblage • Maintenance des appareils et des moyens d'exploitation • Suppression de valeurs • Sécurité des appareils, du matériel d'exploitation et des valeurs à l'extérieur des locaux • Élimination ou réutilisation en toute sécurité des appareils et des moyens d'exploitation • Équipements des utilisateurs sans surveillance • Politique de nettoyage de l'environnement de travail et de verrouillage des écrans	Analyse de la documentation

2.12 Mesures pour la sécurité de l'exploitation	A.5.37 A.8.6 – A.8.8 A.8.13 A.8.15 A.8.17 A.8.19 A.8.31 A.8.32 A.8.34	L'OE dispose-t-elle d'un processus de gestion du changement ? Les environnements de test et d'exploitation sont-ils séparés ? Les exigences en matière de protection contre les logiciels malveillants ont-elles été analysées et des mesures appropriées ont-elles été mises en œuvre ? Existe-t-il des concepts de sauvegarde appropriés et ceux-ci sont-ils régulièrement contrôlés ? Le réseau et les systèmes sont-ils surveillés par des moyens appropriés et les événements sont-ils rendus visibles ? Les scans de vulnérabilité sont-ils effectués régulièrement ? Les vulnérabilités découvertes lors de ces analyses sont-elles corrigées ? Les installations de logiciels sont-elles effectuées selon un processus structuré (c.-à-d. installation uniquement par du personnel formé, documentation de configuration et de système disponible, les nouvelles applications et logiciels sont testés avant d'être introduits, notamment en ce qui concerne les implications en matière de sécurité) ? Un contrôle d'intégrité a-t-il été effectué pour les	Analyse de la documentation Vérification du système

		systèmes d'information nécessitant une protection accrue ? Les systèmes d'information sont-ils régulièrement audités (c.-à-d. au moins une fois par an) et les effets sont-ils minimisés par des mesures d'audit ?	
2.13 Sécurité de la communication (transmission d'informations)			
2.13.1 Documentation architecturale	-	L'OE dispose-t-il d'une documentation sur l'architecture réseau de ses systèmes d'information figurant dans l'inventaire des actifs, qui comprend la topologie de ses propres réseaux et de ceux de tiers ainsi que les composants actifs qui s'y trouvent ?	Analyse de la documentation
2.13.2 Matrice d'accès	-	L'OE dispose-t-il d'une matrice d'accès qui détermine comment les personnes et les processus automatisés (machines/logiciels) peuvent accéder aux systèmes d'information exploités dans les différentes zones du réseau, ou comment ceux-ci doivent être authentifiés et, le cas échéant, autorisés ?	Analyse de la documentation
2.13.3 Sécurité et documentation du réseau	A.5.14 A.6.6 A.8.20 – A.8.22	L'organe d'exécution dispose-t-il de politiques en matière de sécurité des réseaux et celles-ci incluent-elles, entre autres, les responsabilités de gestion des réseaux et	Analyse de la documentation

		des transitions de réseaux ? Existe-t-il un règlement d'utilisation pour les réseaux dont les OE sont responsables, dans lequel sont réglés le raccordement de terminaux de communication étrangers, la réglementation des transitions de réseau ainsi que l'accès à distance ? La structure du réseau est-elle zonée, segmentée et configurée de manière adéquate? Les réseaux sous la responsabilité de l'OE sont-ils surveillés et protégés contre les attaques et les accès non autorisés ? Des mesures de sécurité ont-elles été mises en place pour les réseaux qui ne relèvent pas de la responsabilité de la OE et dont l'utilisation ne peut pas être réglée par contrat (par ex. Internet) ? Toutes les structures du réseau et les responsabilités respectives sont-elles documentées ?	
2.13.4 Transmission protégée des informations	A.5.14 A.6.6	Les données sont-elles suffisamment protégées lors de la transmission d'informations sur des réseaux propres, des réseaux contractuels ou des réseaux étrangers par des mesures appropriées, compte tenu de leur be-	Analyse de la documentation

		soin de protection consigné dans la documentation SIPD ? Les collaborateurs connaissent-ils les différents niveaux de protection lors de la transmission de données et utilisent-ils des moyens de transmission appropriés (par ex. cryptage des courriels, transfert de fichiers sécurisé, etc.)	
2.14 Modifications dans les systèmes d'information	A.5.8 A.8.25 – A.8.27 A.8.29 – A.8.33	La sécurité fait-elle partie intégrante du cycle de vie des systèmes d'information et tient-elle compte des exigences de sécurité spécifiques définies dans la documentation de la SIPD ? La documentation de la SIPD est-elle mise à jour lorsque des modifications sont apportées aux systèmes d'information ou, dans les autres cas, au moins tous les 5 ans ? Existe-t-il un processus pour cela ? La méthode de projet informatique requise par les D-SIPD, cm 2.5, est-elle également appliquée aux modifications des systèmes d'information ? Lors de modifications de systèmes d'information, les exigences définies dans les D-SIPD, paragraphe 2.12, lettre A, point 4, concernant la séparation des environnements de développement, de test et d'exploitation	Analyse de la documentation

		sont-elles prises en compte ? Les données de test générées lors du test de systèmes et de fonctions système sont-elles protégées ?	
2.15 Contrats avec des tiers (relations avec les fournisseurs)	A.5.19 – A.5.21	Les contrats conclus avec des prestataires de services tiers qui ont potentiellement accès à des données relevant du droit des assurances sociales ou qui traitent ces données sur mandat comportent-ils l'obligation de respecter l'ensemble des règles de protection et des exigences concernant concrètement les prestations ? Les contrats prévoient-ils également des mesures de contrôle pour le respect de ces obligations ainsi que des sanctions conventionnelles en cas de violation de ces dispositions ? Les services offerts par des tiers à l'étranger sont-ils identifiés et justifiés ? Est-il garanti qu'aucune donnée personnelle d'assuré n'est traitée à l'étranger ? (Sauf s'il s'agit d'une exception mentionnée dans les D-SIPD, ch. 2.15.1, point 4 [échange international de données]) Les principes du cloud mentionnés dans les D-SIPD ch. 2.15.2 point 5 sont-ils pris en compte	Analyse de la documentation

		lors de l'utilisation de services cloud ?	
2.16 Gestion des incidents de sécurité de l'information	A.5.24 – A.5.28 A.6.8	L'USIC s'assure-t-elle que les notifications d'incidents de sécurité liés aux systèmes d'information sont traitées, documentées et évaluées de manière adéquate afin de minimiser la probabilité d'occurrence ou l'impact d'incidents futurs ? L'organe d'exécution dispose-t-il de plans de réaction et de communication préparés pour les incidents de sécurité, qui garantissent que les mesures appropriées sont prises par les personnes compétentes ?	Analyse de la documentation
2.17 Maintien de la sécurité de l'information (Business Continuity Management BCM)	A.5.29 A.8.14	L'OE dispose-t-il de plans pour maintenir et rétablir le fonctionnement de l'objet de protection SI en cas d'incident, d'urgence ou de catastrophe ? Ces plans sont-ils testés régulièrement, c'est-à-dire au moins 1 fois par an ?	Analyse de la documentation
2.18 Conformité aux directives	A.5.31 – A.5.36 A.8.8	Les éventuelles lacunes identifiées avec le système de contrôle interne (SCI), le système de gestion de la qualité (SMQ) et le système de gestion des risques (GR) en relation avec les systèmes d'information ont-elles été corrigées ? (Indépendamment du fait qu'elles aient déjà été constatées lors d'une révision prudentielle).	Analyse de la documentation