Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Sozialversicherungen BSV

Weisungen zu den Audits über die Informationssicherheit und den Datenschutz (WAID)

Gültig ab 1. Januar 2024

Stand: 20. April 2026

Hinweis
Zur einfacheren Lesbarkeit wurde im gesamten Dokument die männliche Form verwendet. Selbstverständlich sind dabei Personen aller Geschlechter mitgemeint.

d WAID (318.108.09)

01.24

Vorwort

Die Informationssysteme der 1. Säule sollen über die notwendige Stabilität und Anpassungsfähigkeit verfügen sowie die Informationssicherheit und den Datenschutz gewährleisten. Ob die Durchführungsstellen die von der Aufsichtsbehörde festgelegten Anforderungen erfüllen, prüft die Revisionsstelle gestützt auf die BSV-Weisungen (Art. 68a Abs. 2 Bst. c AHVG, Art. 159 Bst. c AHVV und Art. 160 Abs. 5 AHVV).
Das Kapitel 1umfasst sowohl die Anforderungen an die Kompetenz als auch an die Ausbildung der IT-Auditoren.

Das Kapitel 2 umfasst die Anforderungen an den Prüfprozess für das IT-Audit nach Art. 68a Absatz 2 Buchstabe c AHVG. Die Umsetzung der Anforderungen wird einen kontinuierlichen Adaptionsprozess erfordern. Zu diesem Zweck wird ein Reifegradmodell eingeführt, was durch die Revisoren bei ihrer Prüfung zu berücksichtigen ist.

Inhaltsverzeichnis

Abkürzungen 4

Kapitel 1: Anforderungen an die IT-Audit-Verantwortlichen 5

1.1 Praktische Kenntnisse 5
1.2 Ausbildung und Fachkenntnisse 5
1.3 Persönliche Anforderungen 5
1.4 Personensicherheitsprüfung 5
1.5 Prinzipien 6

Kapitel 2: Anforderungen an die IT-Audits 7

2.1 Grundsätze 7
2.2 Auditierte Stellen 7
2.3 Verantwortlichkeiten 8
2.4 Prüfumfang und Ablauf 9
2.5 Berichterstattung 9
2.6 Reifegradmodell 11

Kapitel 3: Inkrafttreten 12

Anhang 1: Fragebogen für IT-Audits 13

1 Prüfhandlungen 13

2 Fragebogen IT-Audit 14

Abkürzungen

AHV	Alters- und Hinterlassenenversicherung
AHVG	Bundesgesetz über die AHV
AHVV	Verordnung über die AHV
ALV	Arbeitslosenversicherung
BSV	Bundesamt für Sozialversicherung
CISA	Certified Information Systems Auditor der ISACA
CISM	Certified Information Security Manager der ISACA
CISSP	Certified Information Systems Security Professional
ISACA	Information Systems Audit and Control Association
ISB	Informationssicherheitsbeauftragter
ISC	International Information Systems Security Certification Consortium
ISMS	Informationssicherheit-Management-System
Rz	Randziffer
TÜV	Technischer Überwachungsverein
ZAS	Zentrale Ausgleichsstelle

Kapitel 1: Anforderungen an die IT-Audit-Verantwortlichen

1.1 Praktische Kenntnisse

1 Die Revisoren beurteilen im Rahmen ihrer Prüfungen, ob die Durchführungsstellen die Anforderungen gemäss Artikel 72a Absatz 2 Buchstabe b AHVG erfüllen. Für das erforderliche Fachwissen weisen die Revisoren praktische Kenntnisse in folgenden Bereichen vor:

- Informationssicherheit;
- Datenschutz;
- IT-Audit.

1.2 Ausbildung und Fachkenntnisse

2 Folgende Anforderungen an die Ausbildung und an die Fachkenntnisse müssen vom IT-Audit-Verantwortlichen erfüllt sein:

- eine abgeschlossene Ausbildung an einer Hochschule, einer Fachhochschule oder einer höheren Fachschule von mindestens einem Jahr Dauer mit Schwerpunkt Informationssicherheit und Datenschutz oder
- eine mindestens zweijährige praktische Tätigkeit im Bereich Informationssicherheit oder IT-Audit als Mitglied von Revisionsteams zugelassener Revisionsgesellschaften. Diese kann auch durch anerkannte Berufszertifizierungen vorgewiesen werden wie beispielsweise:
    - CISA der ISACA oder Lead Auditor des TÜV oder
    - CISM der ISACA bzw. CISSP des ISC.

1.3 Persönliche Anforderungen

3 Die IT-Audit-Verantwortlichen haben keine persönlichen Beziehungen oder Interessen zu der auditierten Stelle. Sie sind unabhängig und unbefangen.

1.4 Personensicherheitsprüfung

4 Der leitende Revisor gemäss Art. 68 Abs. 2 AHVG stellt sicher, dass der IT-Audit-Verantwortliche über einen unbescholtenen Leumund gemäss Art. 5 Abs. 1 Bst. a RAG verfügt.

1.5 Prinzipien

5 Die IT-Audit-Verantwortlichen halten sich an folgende Prinzipien:

- Ethisches Verhalten: Die IT-Audit-Verantwortlichen wahren die Vertraulichkeit der Informationen und Auskünfte;
- Sachliche Darstellung: Die IT-Audit-Verantwortlichen berichten wahrheitsgemäss über die Untersuchungsergebnisse und stellen den Sachverhalt nachvollziehbar dar. Die Prüfungsergebnisse der IT-Audit-Verantwortlichen müssen wiederholbar sein (bei unverändertem Sachstand);
- Angemessene Sorgfalt: Die IT-Audit-Verantwortlichen gehen beim Auditieren sorgfältig um. Deren Urteilsvermögen ist unerlässliche Voraussetzung für sachgerechte und fundierte Audits;
- Nachweise: Die Prüfberichte sind verifizierbar. Die Ergebnisse können auf Stichproben der verfügbaren Informationen beruhen, da ein Audit während eines begrenzten Zeitraumes vorgenommen wird. Die Auswahl der Stichproben ist relevant und wird in einem sinnvollen Umfang vorgenommen.

Kapitel 2: Anforderungen an die IT-Audits

2.1 Grundsätze

6 Das IT-Audit richtet sich nach folgenden Grundsätzen:

- Der Inhalt des Audits basiert auf allgemeinen IT-Kontrollen und stimmt mit der Reihe der international anerkannten und etablierten ISO 27000-Normen überein;
- Das IT-Audit wird risikobasiert durchgeführt;
- Die jährlichen Prüfungen in einem Auditjahr decken die Periode zwischen dem vorangehenden und aktuellen Audit ab. Liegt kein vorheriger Audit als Referenz vor, wird der Stand zum Zeitpunkt des aktuellen Audits geprüft.
- Das BSV kann Prüfungsschwerpunkte festlegen.
- Der IT-Audit-Verantwortliche kann zusätzlich nach seinem Ermessen beim IT-Audit weitere Schwerpunkte setzen.

2.2 Auditierte Stellen

7 Folgende Stellen werden IT-auditiert:

- Alle Durchführungsstellen sofern diese selbst nicht nach ISO 27001 zertifiziert sind oder einen ISAE 3000 Typ1 oder Typ 2 Prüfbericht vorweisen können. Dafür weisen die Durchführungsstellen ihren Zertifizierungs- oder Prüfbericht der Revisionsstelle vor;
- Die Familienausgleichskassen, sofern die Ausgleichskassen die Familienzulagen als übertragene Aufgabe ausrichten;
- Wenn mehrere Ausgleichskassen, die in Personalunion geleitet werden, exakt dieselben Informationssysteme verwenden, genügt ein gemeinsames Audit. Der Auditbericht muss sämtliche betroffenen Ausgleichskassen vollständig abdecken und diese ausdrücklich benennen.
- Dritte, die im Auftrag einer auditierten Durchführungsstelle IT-Dienstleistungen erbringen, potentiell Zugang zu sozialversicherungsrechtlichen Daten haben oder die Bearbeitung über-nehmen (gem. Rz 2.15 W-ISDS), sofern sie nicht ISO 27001 zertifiziert sind, einen ISAE 3000 Prüfbericht Typ 1 oder Typ 2 oder über einen gültigen Auditbericht gemäss Rz 14 WAID verfügen. Ein solcher Auditbericht kann von allen Durchführungsstellen,

die die Leistungen dieses Dritten nutzen und deren Revisionsstellen, als gültiger Nachweis anerkannt werden, sofern er nach den WAID-Vorgaben und von einer Auditstelle erstellt wurde, die den in der WAID festgelegten Anforderungen entspricht. Eine bestehende ISO/IEC-27001-Zertifizierung schliesst nicht aus, dass der Auditor im Rahmen seines pflichtgemässen Ermessens zusätzliche Prüfungshandlungen bei den Dritten vornimmt, sofern dies für die abschliessende Beurteilung relevanter Kontrollen oder Sachverhalte notwendig ist.

Es wird empfohlen, dass Vertragspartner, welche über einen gültigen Auditbericht, eine gültige ISO 27001 Zertifizierung oder einen gültigen ISAE 3000 Prüfbericht verfügen diesen an alle Durchführungsstellen, welche Kunden des entsprechenden Partners sind, übermitteln.

2.3 Verantwortlichkeiten

8 Die Leitung der Durchführungsstelle ist verantwortlich für die Einhaltung der W-ISDS-Anforderungen. Sie stellt sicher, dass der IT-Audit-Verantwortliche seine Aufgabe erfüllen kann, stellt die notwendigen Informationen zur Verfügung und ist gegenüber dem IT-Auditor die Hauptansprechperson.

9 Der Informationssicherheitsbeauftragte der Durchführungsstelle steht dem BSV und dem IT-Audit-Verantwortlichen als Kontaktperson zur Verfügung.

10 Die Revisionsstelle ist für die Durchführung des IT-Audits verantwortlich und kann den entsprechenden Auftrag sowohl intern als auch an externe Dritte erteilen. In Absprache mit der Revisionsstelle kann das IT-Audit auch von der Durchführungsstelle in Auftrag gegeben werden. Die Revisionsstelle bleibt aber verantwortlich. Der IT-Audit-Verantwortliche ist für die Einhaltung der Anforderungen zuständig.

2.4 Prüfumfang und Ablauf

11 Mit der Prüfung der Informationssysteme wird die Verfügbarkeit des ISMS gemäss der W-ISDS kontrolliert.

12 Die Prüfung umfasst folgende Schritte:

- Überprüfung der Massnahmen, die als Reaktion auf das letzte Audit ergriffen wurden;
- Überprüfung der Wirksamkeit der vom ISB definierten Massnahmen im Rahmen des ISMS;
- Bearbeitung des vom BSV standardisierten IT-Audit-Fragebogens (vgl. Anhang 1);
- Erstellung eines IT-Auditberichts (siehe Rz. 14 ff.);
- Überprüfung des IT-Auditberichts durch den ISB der auditierten Stelle und Stellungnahme des ISB zu den vom IT-Audit-Verantwortlichen gerügten Mängeln und vorgeschlagenen Massnahmen;
- Übernahme der Stellungnahme des ISB in den definitiven IT-Auditbericht;
- Zustellung des IT-Auditberichts durch den leitenden Revisor innert Monatsfrist nach Abschluss des IT-Audits gleichzeitig dem Kanton bzw. Gründerverbänden, dem Kassenvorstand, dem BSV, der ZAS und der auditierten Durchführungsstelle.

2.5 Berichterstattung

13 Die IT-Auditberichte sind kurz, eindeutig und kritisch zu verfassen. Sie enthalten alle für die leitenden Organe der Durchführungsstellen sowie den Aufsichtsbehörden wesentlichen Feststellungen. Dabei sind Eigenheiten der jeweiligen Durchführungsstelle aufzuführen und zu berücksichtigen.

14 Der Inhalt der Berichterstattung umfasst mindestens:

- Versionisierungsprotokoll;
- Übersicht/Management Summary;
- Ergebnis des IT-Audits:

1. Zusammenfassung mit Angaben zur auditierten Stelle und Verteiler;
2. Übersicht über die Feststellungen des vorangehenden IT-Audits und dem Stand der Umsetzung der vorgeschlagenen Massnahmen;
3. Aufführung der geprüften IT-Umgebung und der getesteten Kontrollen. Darstellung der Prüfhandlungen und Prüftiefe;
4. Detaillierte Ergebnisse zu den geprüften Punkten je Hauptkapitel der W-ISDS;
5. Ergebnisse der Schwerpunktprüfung;
6. Gesamtbeurteilung;
7. Verbesserungsvorschläge;
8. Der Revisor bestätigt, dass der IT-Audit-Verantwortliche die Anforderungen nach Randziffer 2 und 3 erfüllt;
9. Die IT-Auditoren bestätigen im Prüfbericht, dass sie unabhängig sind und dass die Ergebnisse im Prüfbericht auf eigene Prüfungen beruhen sowie dass sie keine persönlichen Interessen oder Beziehungen zu der auditierten Stelle haben.
10. Der beantwortete IT-Fragebogen gemäss Anhang 1.

Bei der Vorlage einer ISO 27001 Zertifizierung oder eines ISAE 3000 Typ 1 oder Typ 2 Prüfberichts muss die Revisionsstelle Folgendes verifizieren:

- **ISO 27001:**
  - Der Anwendungsbereich des zertifizierten ISMS umfasst alle relevanten Organisationseinheiten und Geschäftsprozesse der Durchführungsstellen
  - In der Anwendbarkeitserklärung des ISMS ist keine der in der W-ISDS geforderten Sicherheitsmassnahmen ausgeschlossen
  - Im (Re-)Zertifizierungs-Audit wurden alle in der W-ISDS geforderten Sicherheitsmassnahmen überprüft.
- **ISAE 3000 Typ 1:**
  - Der Prüfbericht referenziert auf alle festgelegten Anforderungen der Weisung W-ISDS

- **ISAE 3000 Typ 2:**
  - Der Prüfbericht wurde mit hinreichender Sicherheit und zeitraumgeprüft erstellt und nach W-ISDS definierten Kontrollen geprüft.

2.6 Reifegradmodell

15 Die Bewertung der Ergebnisse basiert auf dem IT-Audit-Fragebogen. Der Grad der Konformität wird mit dem Reifegrad der IT-Sicherheitsorganisation der auditierten Stelle wie folgt definiert:

Grad der Erfüllung	Abweichung	Beschreibung	Reifegrad
Erfüllt	Keine	Mit den bestehenden Massnahmen werden die BSV-Anforderungen gemäss den entsprechenden Kontrollen vollständig erreicht.	4
Erfüllt mit Bemerkungen	Keine	Mit den bestehenden Massnahmen werden die BSV-Anforderungen gemäss den entsprechenden Kontrollen vollständig erreicht. Eine Anmerkung wird dennoch gemacht.	3
Teilweise erfüllt	Feststellungen	Mit den bestehenden Massnahmen werden die BSV-Anforderungen gemäss den entsprechenden Kontrollen nur teilweise erreicht.	2
Nicht erfüllt	Feststellungen	Die BSV-Anforderungen gemäss den entsprechenden Kontrollen werden nicht erreicht.	1

Besteht ein begründeter Verdacht, dass eine Durchführungsstelle ihre Pflichten zur Umsetzung der Anforderungen an die Informationssicherheit und den Datenschutz gemäss W-ISDS Randziffern 2.1 bis 2.18 nicht erfüllt

(Reifegrad 1), kann das BSV gestützt auf Art. 72b AHVG geeignete aufsichtsrechtliche Massnahmen anordnen. Dazu gehören insbesondere die Anordnung eines ausserordentlichen Audits auf Kosten der Durchführungsstelle, die Anforderung zusätzlicher Nachweise oder die Festlegung von Massnahmen mit Frist.

Kapitel 3: Inkrafttreten

16 Diese Weisungen treten auf den 1. Januar 2024 in Kraft.

Die ersten IT-Audits werden per 1. Januar 2025 durchgeführt.

Anhang 1: Fragebogen für IT-Audits

1 Prüfhandlungen

Prüfhandlung	Kommentar
Analyse der Dokumentation	Die Anforderung aus der W-ISDS wird mittels Analyse der vorhandenen Dokumentation überprüft. Dabei wird zwischen SOLL- und IST- Dokumentation unterschieden. **SOLL-Dokumentation:** Vorgaben, Richtlinien, Konzepte Pläne, Handlungsanweisungen etc. **IST-Dokumentation:** Nachweise der Umsetzung der SOLL-Dokumentation. Daten-Exporte, Aufzeichnungen (Logs), Protokolle, Screenshots
Systemprüfung	Die Anforderung aus der W-ISDS wird direkt auf dem entsprechenden Informationssystem überprüft. Eine Prüfung am System sollte über einen Zugriff durch den jeweiligen Zuständigen/Verantwortlichen unter Aufsicht des Auditors erfolgen. Als Nachweis können z.B. Screenshots erstellt werden.

2 Fragebogen IT-Audit

Referenz Randziffer (Rz) W-ISDS	**Referenz** ISO 27001:2022	**Fragestellung**	**Erforderliche Prüfhandlung**
2 Anforderungen			
2.1 Informationssicherheits-Management-System ISMS)	4.4	Hat die Durchführungsstelle ein ISMS aufgebaut und im Einsatz?	Analyse der Dokumentation
2.2 Aufbau ISMS			
a) Festlegung sicherheitsrelevanter Themen und Tätigkeiten	4.1	Wurden die sicherheitsrelevanten Themen und Tätigkeiten der DS identifiziert und dokumentiert?	Analyse der Dokumentation
b) Identifikation der dabei involvierten Stellen	4.2	Wurden die für die Informationssicherheit der DS involvierten Stellen identifiziert, dokumentiert?	Analyse der Dokumentation
c) Inventar der Informationssysteme und IT-relevanten Aktivitäten	A.5.9	Wird ein Inventar der Informationssysteme und IT-relevanten Aktivitäten geführt. Wird das Inventar der Informationssysteme regelmässig, d. h. mindestens einmal jährlich aktualisiert? Existiert ein Prozess für die Neuaufnahme/den Austritt von Systemen und IT-Aktivitäten in das Inventar der Informationssysteme?	Analyse der Dokumentation

d) Anwendungsbereich des ISMS ist definiert	4.3	Wurden die Bereiche der DS, welche unter das ISMS fallen, definiert und dokumentiert? Sind allfällige nicht in den Anwendungsbereich des ISMS fallende Bereiche aufgeführt und falls nein, ist die ganze Organisation als Anwendungsbereich angegeben?	Analyse der Dokumentation
e) Das ISMS und seine Komponenten werden regelmässig aktualisiert	4.4	Gibt es sichtbare Handlungen zur laufenden Aktualisierung und Verbesserung des ISMS? [Anm: üblicherweise wird in einem ISMS eine Liste von Verbesserungsopportunitäten geführt und der KVP so dokumentiert und nachvollziehbar gemacht] Gibt es sichtbare Handlungen zur jährlichen Überprüfung der Aktualität des ISMS?	Analyse der Dokumentation
2.3 Informationssicherheitsrichtlinien	A.5.1 A.5.3 A.5.5 A.5.24	Wurden Informationssicherheitsleitlinien erlassen und an die Mitarbeitenden und beauftragte Dritte kommuniziert, welche die aufgeführten Punkte beinhalten?	Analyse der Dokumentation
2.4 Anforderungen an die Informationssicherheitsorganisation	A.5.2	Besteht ein Organigramm der Informationssicherheitsorganisation und wurde es kommuniziert? Wissen die im Organigramm bezeichneten Personen welche Aufgaben sie erfüllen	Analyse der Dokumentation

		müssen und welche Verantwortung sie haben? Hat die DS mindestens eine zentrale Rolle für die Informationssicherheit (z. B. ISB, CISO oder gleichwertig) sowie weitere relevante Rollen benannt und dokumentiert? Sind die Aufgaben der zentralen Rolle sowie der weiteren Personen, die Schlüsselaufgaben in der Umsetzung der Informationssicherheit wahrnehmen, verbindlich dokumentiert (z. B. in Pflichtenheften oder Stellenbeschreibungen)?	
2.5 Anforderungen an Projekte im Bereich Informationssysteme	A.5.8	Besteht eine definierte IT-Projektmanagementmethode, welche den geforderten Punkten entsprechen? Sind IT-Projekte erkennbar, in denen die Projektmanagementmethode angewendet wurde?	Analyse der Dokumentation
2.6 Informationssicherheit bei Mobilgeräten und Mobile Working	A.6.7 A.8.1	Wurde eine Richtlinie zum Mobile Working und Mobilen Geräten / BYOD erstellt und kommuniziert? Enthält diese Richtlinie die in den Weisungen geforderten Elemente?	Analyse der Dokumentation
2.7 Informationssicherheit und Personal			

2.7.1 Personalsicherheit	A.6.1 – A.6.5	Bestehen Weisungen zu Pflichten im Umgang mit Information, Geheimhaltung und IT-Systemen? Werden diese an beauftragte Dritte und das eigene Personal kommuniziert? Besteht ein Prozess zur Rückgabe von Informationen und IT-Mitteln nach Beendigung des Arbeitsverhältnisses von MA bzw. des Auftragsverhältnisses von beauftragten Dritten? Wird eine angemessene Sicherheitsprüfung für MA mit Zugriff auf kritische Informationen, bzw. MA mit privilegierten Zugriffen auf IT-Systeme durchgeführt und periodisch (min. einmal jährlich) aktualisiert? Werden der ISB und weitere Schlüsselrollen der Sicherheitsorganisation spezifisch mit einer Personensicherheitsprüfung überprüft? Beinhaltet die Personensicherheitsprüfung des ISB und weiterer Schlüsselrollen eine Überprüfung des Strafregisters und Betreibungsregisters?	Analyse der Dokumentation
2.7.2 Information und Schulung	A.5.4 A.6.3	Werden mindestens jährlich Schulungen und Sensibilisierungen	Analyse der Dokumentation

	A.6.4	der Mitarbeitenden durchgeführt? Besteht ein Konzept für die Schulung und Sensibilisierung von Mitarbeitenden? Haben die Mitarbeitenden Kenntnis der für sie geltenden Pflichten und Weisungen bezüglich der Informationssicherheit?	
2.7.3 Änderung der Verhältnisse	A.6.5	Besteht ein definierter Prozess zur systematischen Anpassung der Zutritts- und Zugriffsberechtigungen bei Anpassung des Anstellungs- oder Auftragsverhältnisses oder der Nutzervereinbarung? Besteht ein definierter Prozess zur Behandlung unbenutzter Konten und wird dieser befolgt?	Analyse der Dokumentation
2.8 IS-Schutzobjekte: Inventar, ISDS-Dokumentationen und weitere Anforderungen			
2.8.1 Asset Inventar	A.5.9	Werden alle Informationssysteme der DS in einem Inventar geführt und wird das Inventar stets aktuell gehalten?	Analyse der Dokumentation
2.8.2 ISDS-Basisdokumentation	A.5.10 A.5.12 A.5.13	Bestehen ISDS-Dokumentationen für die Projekte und Informationssysteme und entsprechen sie qualitativ und quantitativ dem in der	Analyse der Dokumentation

		W-ISDS Anhang 4 gegebenen Muster? Beinhalten diese Basisdokumentationen die in der W-ISDS unter Rz 2.8.2 Punkt 2 geforderten Elemente pro Informationssystem?	
2.8.3 Erweiterte ISDS-Dokumentation	A.5.10 A.5.12 A.5.13	Wurden für IT-Systeme, mit dem besonders schützenswerte Personendaten bearbeitet werden, erweiterte ISDS-Dokumentationen erstellt, welche die in der W-ISDS unter Rz 2.8.3 definierten Themen beinhalten?	Analyse der Dokumentation
2.8.4 Aktualität der ISDS-Dokumentationen	-	Entsprechen die ISDS-Dokumentationen der betriebenen Informationssysteme den aktuellen Verhältnissen?	Analyse der Dokumentation
2.8.5 Anwendungsverantwortlicher	A.5.9	Ist im Asset-Inventar für jedes Schutzobjekt eine verantwortliche Person bestimmt worden? Haben diese Personen Kenntnis von ihren Verantwortlichkeiten?	Analyse der Dokumentation
2.9 Zugriffssteuerung zu den Informationssystemen	A.5.15 – A.5.18 A.8.2 – A.8.5	Existiert ein dokumentiertes Zugriffssteuerungskonzept, welches wenigstens die in der W-ISDS Rz 2.9 aufgelisteten Punkte beinhaltet? Sind alle Zugriffe (inkl. automatisierten Prozessen mit machine-to-machine-Zugriff) auf	Analyse der Dokumentation Systemprüfung

		Informationssysteme mit einer dem Schutzbedarf entsprechenden Authentifikation und nötigenfalls adäquaten kryptographischen Massnahmen gemäss der definierten Zugriffsmatrix geschützt? Wird für die Zugriffe das Prinzip des «least privilege» umgesetzt? Werden die Zugriffe auf besonders schützenswerte Personendaten gemäss Art. 4 DSV protokolliert? Werden die Richtigkeit und Zweckmässigkeit der Zugriffe mindestens jährlich geprüft?	
2.10 Kryptographie			
2.10.1 Kryptographische Methoden und Verfahren	A.8.24	Entsprechen die eingesetzten kryptographischen Verfahren und Methoden den anerkannten Regeln der Technik? Werden beim Einsatz von Schlüsselzertifikaten dieselben, abhängig vom jeweiligen Anwendungsfall und den damit verbundenen gesetzlichen Anforderungen, von einer anerkannten Certificate Autorithy (CA) ausgestellt? Werden die kryptographischen Schlüssel sicher verwaltet und wird deren Gültigkeit sichergestellt?	Analyse der Dokumentation Systemprüfung

2.11 Physischer Schutz			
2.11.1 Sicherheitsdispositiv für Räumlichkeiten	A.7.1 – A.7.3 A.7.5	Sind die Informationssysteme mit gemäss ihrer zugewiesenen Schutzgruppe adäquaten physischen Schutzmassnahmen geschützt? • Physische Sicherheitsperimeter (Lage der Umgebung und bauliche Massnahmen) • Physische Zutrittssteuerung • Sichern von Büros, Räumen und Einrichtungen • Schutz vor externen und umweltbedingten Bedrohungen	Analyse der Dokumentation
2.11.2 Massnahmen für Geräte und Betriebsmittel	A.7.7 – A.7.14 A.8.1	Sind die folgenden Massnahmen zum Schutz von Geräten und Betriebsmitteln angemessen umgesetzt? • Platzierung und Schutz von Geräten und Betriebsmitteln • Versorgungseinrichtungen • Sicherheit der Verkabelung • Instandhalten von Geräten und Betriebsmitteln • Entfernen von Werten • Sicherheit von Geräten, Betriebsmitteln und Werten	Analyse der Dokumentation

		ausserhalb der Räumlichkeiten • Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln • Unbeaufsichtigte Benutzergeräte • Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren	
2.12 Massnahmen für die Betriebssicherheit	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	Verfügt die DS über einen Change-Management Prozess? Sind Entwicklungs- Test- und Betriebsumgebungen getrennt voneinander? Sind Anforderungen zum Schutz vor Malware analysiert und geeignete Massnahmen umgesetzt worden? Bestehen geeignete Backup-Konzepte und werden diese regelmässig überprüft? Wird das Netzwerk und die Systeme mit geeigneten Mitteln überwacht und werden Ereignisse sichtbar gemacht? Werden Vulnerability Scans regelmässig durchgeführt? Werden die dabei entdeckten Schwachstellen behoben?	Analyse der Dokumentation Systemprüfung

		Werden Softwareinstallationen gemäss einem strukturierten Prozess durchgeführt (d.h. Installation nur durch geschultes Personal, Konfigurations- und Systemdokumentationen vorhanden, Neue Applikationen und Software wird vor Einführung getestet, insbesondere auf Sicherheitsimplikationen)? Wurde bei Informationssystemen mit einem erhöhten Schutzbedarf eine Integritätsprüfung durchgeführt? Werden die Informationssysteme regelmässig auditiert (d.h. min. einmal jährlich) und die Auswirkungen mittels Auditmassnahmen entsprechend minimiert?	
2.13 Kommunikationssicherheit (Informationsübertragung			
2.13.1 Architekturdokumentation	-	Verfügt die DS über eine Dokumentation der Netzwerkarchitektur ihrer im Asset Inventar geführten Informationssysteme, welche die Topologie der eigenen und fremden Netzwerke und die darin befindlichen aktiven Komponenten umfasst?	Analyse der Dokumentation
2.13.2 Zugriffsmatrix	-	Verfügt die DS über eine Zugriffsmatrix, die	Analyse der Dokumentation

		festlegt, wie Personen und automatisierte Prozesse (Maschinen/Software) auf die in den verschiedenen Netzzonen betriebenen Informationssysteme zugreifen können, bzw. wie diese zu authentifizieren und allenfalls auch zu autorisieren sind?	
2.13.3 Netzwerksicherheit und -dokumentation	A.5.14 A.6.6 A.8.20 – A.8.22	Verfügt die Durchführungsstelle über Richtlinien zur Netzwerksicherheit und beinhalten diese unter anderem die Zuständigkeiten der Verwaltung von Netzwerken und Netzwerkübergängen? Besteht ein Nutzungsreglement zu den von den DS verantworteten Netzwerken in dem der Anschluss von fremden Kommunikationsendgeräten, die Regelung der Netzübergänge sowie der Remote Access geregelt ist? Ist die Netzwerkstruktur adäquat zoniert, segmentiert und konfiguriert? Werden die Netzwerke in der Verantwortlichkeit der DS überwacht und vor Angriffen und unberechtigten Zugriffen geschützt? Sind für Netze, welche nicht in den Verantwortlichkeitsbereich der DS liegt und deren	Analyse der Dokumentation

		Nutzung nicht vertraglich geregelt sein kann (z.B. Internet), Sicherheitsmassnahmen umgesetzt? Sind alle Netzwerkstrukturen und die jeweiligen Zuständigkeiten dokumentiert?	
2.13.4 Geschützte Informationsübertragung	A.5.14 A.6.6	Werden die Daten bei der Informationsübertragung über eigene Netze, vertraglich geregelte Netze oder fremde Netze mit geeigneten Massnahmen unter Berücksichtigung ihres in der ISDS-Dokumentation festgehaltenen Schutzbedarfs, ausreichend geschützt? Sind die verschiedenen Schutzniveaus bei der Datenübermittlung bei den Mitarbeitenden bekannt und Nutzen die Mitarbeitenden entsprechend geeignete Übertragungsmittel? (z.B. E-Mail-Verschlüsselung, gesicherter File-Transfer, usw.).	Analyse der Dokumentation
2.14 Änderungen an Informationssystemen	A.5.8 A.8.25 – A.8.27 A.8.29 – A.8.33	Ist die Sicherheit über den gesamten Lebenszyklus von Informationssystemen hinweg fester Bestandteil und werden dabei die spezifischen, in der ISDS-Dokumentation definierten Sicherheitsanforderungen berücksichtigt?	Analyse der Dokumentation

		Werden die ISDS-Dokumentationen bei Veränderungen an Informationssystemen oder ansonsten mindestens alle 5 Jahre aktualisiert? Existiert dazu ein Prozess? Wird die gemäss W-ISDS Rz 2.5 geforderte IT-Projekt-Methode auch bei Änderungen an Informationssystemen angewendet? Werden bei Änderungen an Informationssystemen die gemäss W-ISDS Rz 2.12 Bst. A, Punkt 4 definierten Anforderungen hinsichtlich Trennung von Entwicklungs-, Test- und Betriebsumgebungen berücksichtigt? Werden Testdaten, die beim Testen von Systemen und Systemfunktionen anfallen, geschützt?	
2.15 Verträge mit Dritten (Lieferantenbeziehungen)	A.5.19 – A.5.21	Beinhalten die Verträge mit Dritten Dienstleistungserbringerinnen, die potenziellen Zugang zu sozialversicherungsrechtlichen Daten haben oder diese Daten im Auftrag bearbeiten, die Verpflichtung zur Einhaltung sämtlicher Schutzvorschriften und der die Leistungen konkret betreffenden Anforderungen?	Analyse der Dokumentation

		Beinhalten die Verträge ebenfalls Kontrollmassnahmen zur Einhaltung dieser Verpflichtungen sowie Konventionalstrafen für den Fall der Verletzung dieser Vorschriften? Sind Dienstleistungen, die von Dritten im Ausland angeboten werden, ausgewiesen und begründet? Wird sichergestellt, dass keine Personendaten von Versicherten im Ausland bearbeitet werden? (Ausser es handelt sich um eine in der W-ISDS Rz 2.15.1 Punkt 4 erwähnte Ausnahme (internationaler Datenaustausch)) Werden bei der Nutzung von Cloud-Diensten die in der W-ISDS Rz 2.15.2 erwähnten Cloud-Prinzipien berücksichtigt?	
2.16 Management von Informationssicherheitsvorfällen	A.5.24 – A.5.28 A.6.8	Stellt der ISB sicher, dass Meldungen über Sicherheitsvorfälle in Zusammenhang mit Informationssystemen adäquat bearbeitet, dokumentiert und ausgewertet werden, um die Eintrittswahrscheinlichkeit oder die Auswirkungen von künftigen Vorfällen zu minimieren?	Analyse der Dokumentation

		Verfügt die Durchführungsstelle über vorbereitete Reaktions- und Kommunikationspläne für Sicherheitsvorfälle, welche sicherstellen, dass die geeigneten Massnahmen durch die zuständigen Personen getroffen werden?	
2.17 Aufrechterhaltung der Informationssicherheit (Business Continuity Management BCM)	A.5.29 A.8.14	Verfügt die DS über Pläne, um bei Störfällen, Notfällen und Katastrophenfällen den Betrieb des IS-Schutzobjektes aufrechtzuerhalten und wiederherzustellen? Werden diese Pläne regelmässig, d.h. mindestens einmal jährlich getestet?	Analyse der Dokumentation
2.18 Richtlinienkonformität	A.5.31 – A.5.36 A.8.8	Wurden allfällige mit dem IKS, QMS und RM erkannte Mängel im Zusammenhang mit den Informationssystemen behoben? (unabhängig davon, ob diese bereits in einer aufsichtsrechtlichen Revision festgestellt worden sind.)	Analyse der Dokumentation