Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Staatssekretariat für Wirtschaft SECO
Interne Revision

Notiz – Review zum ISMS-Konzept

Datum:	12.08.2026
Referenz:	2026-04
Für:	Direktorin SECO, Leiter RS, ISBO SECO, ISBO TC
Kopie an:	Leiter RSIM, Leiter TC, Leiter TCIT, Stv. Leiter Stab DB, Leiterin Governance und Führungsunterstützung Ressourcen GS-WBF, Mandatsleiter EFK

Die Informationssicherheitsverordnung[1] (ISV) verpflichtet das SECO per Ende 2026 zur Einführung eines Informationssicherheits-Managementsystems (ISMS). Unser Jahresprüfprogramm für das Jahr 2026, das vom GL-A SECO genehmigt worden ist, enthält die Durchführung einer Review zum ISMS-Konzept des SECO.

Ziele unserer Review ist das ISMS-Konzept des SECO zu analysieren und beurteilen, ob alle wesentlichen Aspekte (einschliesslich der gesetzlichen Anforderungen[2]) der Informationssicherheit zweckmässig berücksichtigt werden.

Wir haben zur Durchführung der Analyse folgende übergeordnete Prüfobjekte festgelegt:

- Governance, Steuerung und Weiterentwicklung im Bereich ISMS
- ISMS-Konzeptgestaltung und -Methodik (konzeptionelle Angemessenheit)
- Rechtliche Konformität (Compliance)
- Realisierbarkeit und Wirtschaftlichkeit des ISMS

Zu jedem Prüfobjekt bestehen Prüfpunkte bzw. Prüfziele, die eine angemessene Review des ISMS und insbesondere des ISMS-Konzepts ermöglichen. Die Feststellungen zu den einzelnen Prüfzielen sind hier unten ab S. 3 aufgeführt. Für jedes identifizierte Verbesserungspotenzial bzw. Nettorisiko wurde im Rahmen der Empfehlung 1 ein entsprechender Verbesserungsvorschlag formuliert (siehe Anhang 2). Wir haben zudem eine separate Empfehlung zur Ressourcensituation im Bereich ISMS formuliert. Die Empfehlungen und die Stellungnahmen befinden sich im Anhang 1.

Die Prüfungsaktivitäten erfolgten in Übereinstimmung mit den verbindlichen Elementen[3] der Internationalen Grundlagen für die berufliche Praxis des Institute of Internal Auditors (IIA). Als Referenz zur Überprüfung der Inhalte des ISMS-Konzepts haben wir die internationale Norm

[1] Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (ISV) vom 8. November 2023, SR 128.1

[2] Die Einhaltung der Artikel 4 bis 14 der ISV steht hier im Prüffokus.

[3] Global Internal Audit Standards und Topical Requirements.

ISO/IEC 27001 (und entsprechender Anhang) berücksichtigt, die die Anforderungen für Erstellung, Einführung, Betrieb, Überwachung, Wartung, Verbesserung und Compliance eines dokumentierten ISMS umschreibt.

Die Review wurde im Mai 2026 in der Form einer Dokumentenprüfung durchgeführt und hat sich grundsätzlich auf die aktuelle Fassung des ISMS-Konzepts beschränkt. Die Angemessenheit und Wirksamkeit der operativen Umsetzung der einzelnen Vorgaben bzw. Prozesse wurden nicht geprüft.

Die Ergebnisse der Überprüfung und die Empfehlungen wurden der InfoSec Organisation unter der Leitung des Informationssicherheitsverantwortlichen (ISVV) vorab schriftlich zur Abstimmung und Stellungnahme vorgelegt. Eine Sitzung mit den Geprüften zur Abstimmung der Prüfergebnisse hat am 18. Juni 2026 stattgefunden. Die Stellungnahmen zu den Empfehlungen wurden berücksichtigt und in den Bericht aufgenommen. Die Ergebnisse der Prüfung wurden am 12. August 2026 besprochen. Bei dieser Schlussbesprechung nahmen teil:

ISVV und Leiter RS

Leiter a.i. Interne Revision

Wir danken allen involvierten Mitarbeitenden für die wertvolle, konstruktive und kooperative Zusammenarbeit.

Staatsekretariat für Wirtschaft
Interne Revision SECO

Leiter a.i. Interne Revision

Stv. Leiter a.i. Interne Revision

Feststellungen

1. Governance, Steuerung und Weiterentwicklung im Bereich ISMS

1.1. Organisation, Rollen, Integration und Steuerung

Prüfziel 1	Prüfen, ob • die Rollen und Verantwortlichkeiten klar und sauber zugewiesen sind; • die Trennung von 1st- und 2nd-Line klar geregelt ist; • keine Doppelspurigkeiten oder Lücken in den Zuständigkeiten bestehen.
Status[4]	**Feststellungen und Einschätzung IR SECO**
●	<u>Positive Elemente</u> • Angemessene Governance bzw. organisatorische Struktur mit definierten strategischen, taktischen und operativen Ebenen. • Klar definierter Scope der InfoSec-Organisation mit Abdeckung des gesamten SECO. • Zentrale Rollen auf strategische und taktische Ebene formalisiert, dokumentiert und sauber zugewiesen (inkl. Stellvertretungen). Trennung von 1st- und 2nd-Line angemessen geregelt. Zuständigkeiten klar auf die verschiedenen Rollen aufgeteilt. <u>Verbesserungspotenzial (Nettorisiken)</u> • ISMS-Aufgaben noch nicht in den Stellenbeschreibungen verankert. Es besteht die Gefahr, dass die Aufgaben nicht korrekt wahrgenommen werden und die Verantwortungen nicht korrekt getragen werden. Zudem könnte eine neue Evaluation der Lohnklasse nötig sein, da zusätzliche AKV für die Informationssicherheit in den Stellenbeschreibungen ergänzt werden. *(1)*[5] • Rollen und Verantwortlichkeiten im Bereich «*Operative Sicherheit*» definiert aber noch nicht sauber zugewiesen. *(2)* • Zusammensetzung des Steuerungsgremiums «*IT-Security Board*» nicht klar definiert. *(3)*

[4] Legende: ● = angemessen; ● = verbesserungswürdig

[5] Bezug auf die Empfehlung 1 (siehe Anhang 1) bzw. auf die Liste mit den Verbesserungsvorschlägen (siehe Anhang 2).

Prüfziel 2	Prüfen, ob die Einbindung der Geschäftsleitung ausreichend definiert ist.
Status	**Feststellungen und Einschätzung IR SECO**
●	Der GL-A SECO hat per 1. Januar 2026 das IKT-Organisationsreglement des SECO aktualisiert, um die Sicherheitsorganisation sowie die entsprechenden Verantwortlichkeiten im Bereich Sicherheit im IKT-Organisationsreglement zu verankern. Die Informationssicherheit und das ISMS werden somit explizit auf Stufe IT-Governance berücksichtigt. Die Einbindung der GL zum Thema ISMS ist ausreichend definiert und der ISVV (Leiter Ressourcen und Mitglieder GL-A SECO) kann dies sicherstellen. Eine Berichterstattung an GL-A SECO ist vorgesehen.

Prüfziel 3	Prüfen, ob ausreichende Schnittstellen zu IT-Governance, Risikomanagement, BCM und ITSCM bestehen.
Status	**Feststellungen und Einschätzung IR SECO**
●	<u>Positive Elemente</u> • Das ISMS ist im IKT-Organisationsreglement verankert und damit auf Ebene der IT-Governance berücksichtigt. <u>Verbesserungspotenzial (Nettorisiken)</u> • Die Berichterstattung zu IT-Risiken an das unternehmensweite Risikomanagement ist noch nicht ausreichend definiert. *(4)* • BCM ist in den Vorgaben berücksichtigt; konkrete Informationen zur Zusammenarbeit zwischen CISO/ISBO und BCM-Verantwortlichen des SECO liegen jedoch nicht vor. Ein Bestandteil der Schutzbedarfsanalyse ist die Festlegung der BCM-Relevanz des mit dem jeweiligen Schutzobjekt verbundenen Geschäftsprozesses. Aus unserer Sicht sollte hierfür ein standardisierter Austausch zwischen dem ISBO und dem BCM-Verantwortlichen des SECO vorgesehen und im ISMS-Konzept konkret geregelt werden. *(5)* • Für BCM-relevante Schutzobjekte sind auch aus IT-Sicht die entsprechenden ITSCM-Anforderungen zu definieren. Die daraus resultierenden Anforderungen bzw. vereinbarten Servicelevels werden in der Regel in SLAs (Service Level Agreements) und/oder OLAs (Operational Level Agreements) festgehalten. Die Geschäftskontinuität ist ebenfalls Teil der Sicherheitsprozesse der Bundesverwaltung und ist im Rahmen des Grundschutzes IKT und bei Bedarf auch anhand eines Notfallkonzeptes sicherzustellen. Aktuell sind keine detaillierten Informationen dazu in den ISMS-Weisungen zu finden. *(6)*

1.2. Kontinuierliche Verbesserung, Ziele, Key Performance Indicators (KPIs) und Management-Review

Prüfziel 4	Prüfen, ob Ziele, KPIs und Reportingprozesse festgelegt bzw. vorgesehen sind.
Status	**Feststellungen und Einschätzung IR SECO**
●	Positive Elemente • Strategische und operative Sicherheitsziele wurden definiert. Aufgaben zur Zielerreichung sind festgelegt. Die Beurteilung der Zielerreichung sowie die Messung der KPIs sind Bestandteil des vorgesehen Reportingprozesses. • Es bestehen Richtlinien für die Berichterstattung sowie das Management Review, welche ein halbjährliches Reporting an die Hierarchie (ISVV und GL-A SECO) sowie eine jährliche Überprüfung des ISMS des SECO vorsehen. Verbesserungspotenzial (Nettorisiken) Konkrete KPIs wurden noch nicht definiert. Zudem erscheinen einzelne Ziele nur teilweise operationalisierbar. *(7)*

Prüfziel 5	Prüfen, ob ein strukturierter Review-Zyklus und eine kontinuierliche Verbesserung des ISMS vorgesehen sind.
Status	**Feststellungen und Einschätzung IR SECO**
●	Positive Elemente • Ein Reporting- und Reviewprozess wurde definiert (vgl. auch Prüfziel 4). • Ein Prozess zur kontinuierlichen Verbesserung wurde festgelegt. • Ein jährlicher Kontroll- und Auditplan sowie eine Überprüfung durch eine unabhängige Stelle (alle drei Jahre) sind vorgesehen. Verbesserungspotenzial (Nettorisiken) Die Wirksamkeit des ISMS basiert wesentlich auf dem kontinuierlichen Verbesserungsprozess im Sinne des PDCA-Zyklus[6]. Aus unserer Sicht ist derzeit fraglich, ob dieser Prozess mit den aktuell begrenzten Ressourcen angemessen sichergestellt werden kann (derzeit rund 2.6 FTE

[6] Plan-Do-Check-Act.

	für Kontrollfunktionen auf taktischer Ebene im Bereich Informationssicherheit). Gemäss den Angaben der ISBO sollen drei zusätzliche Stellen besetzt werden, wodurch sich die Situation verbessern sollte. Nach den uns vorliegenden Informationen scheint es jedoch Schwierigkeiten bei der Rekrutierung zu geben. Bereits im Rahmen des Audits zur Reaktionsfähigkeit auf Cyberangriffe Mitte 2025 (Ref. 2025-intern-02) wurde uns mitgeteilt, dass 4–5 Personen im Bereich InfoSec rekrutiert werden sollen. Bis heute wurde jedoch lediglich ein Äquivalent von 1.4 FTE besetzt. Das SECO sollte die Situation im Verlauf der zweiten Jahreshälfte 2026 sowie insbesondere im Jahr 2027 eng beobachten und bei Bedarf eine weitere Erhöhung der Ressourcen prüfen. Es besteht das Risiko, dass ein Managementsystem eingeführt bzw. in Gang gesetzt wird, dem anschliessend die notwendigen Ressourcen zur nachhaltigen Wirkungserzielung fehlen. Siehe **Empfehlung 2**.

2. ISMS-Konzeptgestaltung und -Methodik (konzeptionelle Angemessenheit)

2.1. Vollständigkeit, Kohärenz und Verständlichkeit

Prüfziel 6	Prüfen, ob der Geltungsbereich des ISMS sauber definiert ist.
Status	**Feststellungen und Einschätzung IR SECO**
●	Der Geltungsbereich des ISMS ist sauber definiert. Das ISMS gilt für sämtliche Mitarbeitenden des SECO an sämtlichen Standorten und verpflichtet die verantwortlichen Stellen sicherzustellen, dass die entsprechenden Vorgaben auch von externen Personen wie insbesondere, jedoch nicht abschliessend, externen Fachpersonen, Beratern, Dienstleistern, Besuchern sowie weiteren Personen mit Zutritt zu den Räumlichkeiten des SECO verbindlich eingehalten werden.

Prüfziel 7	Prüfen, ob die wesentlichen ISMS-Elemente und -Prozesse gemäss ISO/IEC 27001 ausreichend beschrieben sind.
Status	**Feststellungen und Einschätzung IR SECO**
●	<u>Positive Elemente</u> **Asset Management**, **Risikomanagement**, **Physische Sicherheit**, **Berechtigungsmanagement** und **Kryptografie** sind angemessen berücksichtigt.

	Verbesserungspotenzial (Nettorisiken)
	• **Operations Security**, **Vorfallmanagement** und **Incident Management** (bzw. Krisenmanagement bei wesentlichen Ereignissen) sind berücksichtigt, dennoch bestehen in einzelnen untergeordneten Aspekten Verbesserungspotenziale:
	  ○ Der Change-Management-Prozess ist weder vollständig ausgearbeitet noch formalisiert. *(8)*
	  ○ Für ITSCM vgl. Ausführungen beim Prüfziel 3.
	• Hinsichtlich des **Lieferantenmanagements** werden mehrere zentrale Themen, wie die Incident-Bewältigung und Kontrollrechte, im ISMS-Konzept geregelt. Für die konkrete Ausgestaltung der Anforderungen an Lieferanten wird überwiegend auf die Verträge verwiesen. Entsprechend behandeln die Richtlinien gewisse wesentliche Aspekte nicht ausreichend, insbesondere die Vertraulichkeit beim Informationsaustausch, die sichere Rückgabe und Löschung von Informationswerten bei externen IT-Dienstleistungen sowie die konkreten Schutzanforderungen für Informationen in solchen externen IT-Diensten. *(9)*

Prüfziel 8	Prüfen, ob die Struktur des ISMS-Konzepts klar aufgebaut ist, ob Begriffe und Definitionen einheitlich verwendet werden sowie ob das ISMS-Konzept klar formuliert und adressatengerecht ausgestaltet ist.
Status	**Feststellungen und Einschätzung IR SECO**
●	Die Struktur des ISMS-Konzepts ist klar. Die Dokumentation verwendet klare Begriffe und Definitionen, welche dem Zielpublikum ein angemessenes Verständnis der Inhalte ermöglichen kann. Es handelt sich in jedem Fall um ein eher technisches Thema, und Grundkenntnisse im Bereich Informationssicherheit und Informatik sind notwendig, um den Inhalt bestmöglich zu verstehen.

2.2. Risikomanagement

Prüfziel 9	Prüfen, ob das Risikomanagement im Bereich ISMS angemessen konzipiert ist.
Status	**Feststellungen und Einschätzung IR SECO**

●	Es besteht ein formalisiertes Verfahren zur Identifikation, Bewertung und Steuerung von Informationssicherheitsrisiken. Sowohl periodische als auch ereignisbezogene Risikobewertungen sind vorgesehen. Die Kriterien für die Zuweisung von Verantwortlichkeiten (z.B. Risk Owner) sind definiert. Der Risikomanagement-Prozess beschreibt in angemessener Weise die Definition, Dokumentation und Überprüfung der Risikobehandlungsmassnahmen sowie die Führung des entsprechenden Massnahmenplans und die Nachverfolgung des Umsetzungsstatus.

2.3. Umsetzbarkeit

Prüfziel 10	Prüfen, ob die Vorgaben im ISMS-Konzept operationalisierbar sind.
Status	**Feststellungen und Einschätzung IR SECO**
●	Positive Elemente Die Prozesse zur Bewertung der Erreichung der Ziele, zum Reporting, zur kontinuierlichen Verbesserung, zum Asset Management, zum Risikomanagement, zur Erstellung und Umsetzung des jährlichen Kontroll- und Auditplans (sowie der unabhängigen externen Audits) und zur Schulung der Mitarbeitenden erscheinen grundsätzlich angemessen operationalisierbar. Verbesserungspotenzial (Nettorisiken) • Das Lieferantenmanagement erscheint aktuell noch nicht genügend konkret (vgl. Prüfziel 7). • Für die Aktualisierung der Referenzdokumentation, insbesondere der Liste der Rechtsgrundlagen, des Inventars der Schutzobjekte und der Ausnahmeliste, besteht derzeit kein definierter Prozess. *(10)* • Der Prozess zum Incident Management befindet sich noch in Erarbeitung (vgl. Prüfziel 12).

Prüfziel 11	Prüfen, ob konkrete Mindestanforderungen und Verbindlichkeiten vorhanden sind.
Status	**Feststellungen und Einschätzung IR SECO**
●	Das ISMS-Konzept wurde auf Grundlage der Normen ISO/IEC 27001 und 27002 erarbeitet. Jedes Kapitel der Weisungen verweist auf die jeweilige Anforderung der ISO Normen sowie auf die gesetzlichen Grundlagen (Mindestanforderungen gemäss ISV). Diese Systematik

	gewährleistet eine konsistente und transparente Verknüpfung zwischen internationalen Standards und nationalen regulatorischen Anforderungen. Gleichzeitig dient sie der rechtssicheren Dokumentation sowie der klaren Nachvollziehbarkeit der Compliance-Pflichten des SECO. Um die Einhaltung der verschiedenen Anforderungen sicherzustellen, regelt eine Richtlinie die Konsequenzen bei Verstössen. Vorgesehen sind insbesondere erneute Schulungen zum nicht eingehaltenen Themenbereich sowie, bei wiederholter Nichteinhaltung, disziplinarische und/oder arbeitsrechtliche Massnahmen. Dank der bei der Dokumentenerstellung angewandten Systematik kann u. E. die Einhaltung der minimalen gesetzlichen Anforderungen rasch überprüft werden. Die vorgesehenen Konsequenzen bei Verstössen gegen die Richtlinien tragen zusätzlich dazu bei, die Mitarbeitenden für die Bedeutung dieser Vorgaben zu sensibilisieren und ihre Eigenverantwortung zu stärken.

3. Rechtliche Konformität (Compliance)

Prüfziel 12	Prüfen, ob die gesetzlichen Anforderungen (Artikel 4 bis 14 der ISV) vollständig und korrekt berücksichtigt sind.	
Status	**Feststellungen und Einschätzung IR SECO**	
●	Art. 4 ISV	Das ISMS-Konzept entspricht vollständig den gesetzlichen Anforderungen.
●	Art. 5 ISV	Verbesserungspotenzial (Nettorisiken) Das ISMS-Konzept erfüllt die gesetzlichen Anforderungen gemäss Art. 5 Abs. 1–3 ISV vollständig, jene gemäss Abs. 4 jedoch nur teilweise: Es bestehen Verweise auf eine Weisung zum Risikomanagement sowie auf ein BCM-Dokument, jedoch noch nicht auf ein spezifisches Dokument zum Krisenmanagement. *(11)*
●	Art. 6 ISV	Positive Elemente Das ISMS-Konzept sieht eine Auflistung der für die Informationssicherheit relevanten gesetzlichen Grundlagen vor und weist den Mitarbeitenden die Verantwortung für die Einhaltung der entsprechenden Vorgaben zu. Verbesserungspotenzial (Nettorisiken)

		Es sind keine Richtlinien definiert, wie die Liste der relevanten gesetzlichen Grundlagen sowie allfälliger vertraglicher Verpflichtungen zu führen, zu überprüfen und aktuell zu halten ist (vgl. Prüfziel 10). Der Aspekt der vertraglichen Verpflichtungen wird nicht ausdrücklich berücksichtigt. *(12)*
🟡	Art. 7 ISV	Verbesserungspotenzial (Nettorisiken) Das ISMS-Konzept erfüllt die gesetzlichen Anforderungen, indem es einen spezifischen Anhang zu den Schutzobjekten vorsieht. Dieser befindet sich derzeit jedoch noch in Erarbeitung. *(13)*
🟢	Art. 8 ISV	Das ISMS-Konzept entspricht vollständig den gesetzlichen Anforderungen.
🟡	Art. 9 ISV	Verbesserungspotenzial (Nettorisiken) Das ISMS-Konzept und den dazugehörenden Dokumenten enthalten derzeit kein Verweis auf Art. 9 ISV. *(14)*
🟢	Art. 10 ISV	Das ISMS-Konzept entspricht vollständig den gesetzlichen Anforderungen.
🟡	Art. 11 ISV	Verbesserungspotenzial (Nettorisiken) Das ISMS-Konzept erfüllt die gesetzlichen Anforderungen gemäss Art. 11 Abs. 1 und 3 ISV vollständig, jene gemäss Abs. 2 jedoch nur teilweise: Die Inhalte der Schulungen umfassen sämtliche vorgesehenen Themen, mit Ausnahme der Kontrollaufgaben der Vorgesetzten. *(15)*
🟡	Art. 12 ISV	Positive Elemente Das ISMS-Konzept entspricht den Anforderungen von Art. 12 Abs. 2 ISV. Die Bestimmung richtet sich primär an die Leistungserbringer. Zu diesem Zweck regelt eine Richtlinie des ISMS-Konzepts die Bewirtschaftung von Sicherheitsvorfällen durch die Leistungserbringer einschliesslich der Meldepflichten. Verbesserungspotenzial (Nettorisiken) Das ISMS-Konzept enthält ein Kapitel zum Security Incident Management und verweist auf die noch zu erstellende *Prozessbeschreibung Security Incident Management ISMS*. Gemäss Aufbau und Verweisen erscheint es plausibel, dass darin die weiteren Anforderungen von Art. 12 ISV adressiert werden. *(16)*

●	Art. 13 ISV	Das ISMS-Konzept entspricht vollständig den gesetzlichen Anforderungen.
●	Art. 14 ISV	Das ISMS-Konzept entspricht vollständig den gesetzlichen Anforderungen.

4. Realisierbarkeit und Wirtschaftlichkeit des ISMS

Prüfziel 13	Prüfen, ob das konzipierte ISMS nicht zu komplex oder zu ambitioniert gestaltet ist.
Status	**Feststellungen und Einschätzung IR SECO**
●	Nach eingehender Analyse der bereits vorliegenden Dokumentation (übergeordnete Weisungen bzw. Richtlinien und dazugehörende Dokumente), die in den kommenden Jahren laufend aktualisiert und weiterentwickelt werden sollen, kann durchaus der Eindruck entstehen, dass es sich um ein komplexes Managementsystem für das SECO handelt. Die Dokumentation wurde auf der Grundlage der Norm ISO/IEC 27001 erstellt, welche aufgrund ihres risikobasierten Ansatzes sowie der Vielzahl an technischen, organisatorischen, personellen und physischen Sicherheitsmassnahmen intrinsisch komplex ist. Ein ISMS nach ISO 27001 ist daher zwangsläufig anspruchsvoll und ambitioniert ausgestaltet. Dies entspricht jedoch der hohen Bedeutung der Informationssicherheit in grossen Organisationen. Die Einführung eines ISMS ist zudem als iterativer Prozess zu verstehen. Aktuell befindet sich das Vorhaben primär in der Phase der Definition und Formalisierung von Weisungen, Prozessen und Dokumentationen. Ob das ISMS tatsächlich wirksam funktioniert und einen konkreten Mehrwert für die Informationssicherheit schafft, kann jedoch erst durch die praktische Anwendung sowie durch regelmässige Kontrollen seitens der ISO und ISBO/CISO sowie durch unabhängige Audits beurteilt werden. Ohne eine systematische Überprüfung der Einhaltung der definierten Vorgaben besteht das Risiko, dass das konzipierte ISMS hauptsächlich auf formeller Ebene besteht und seine beabsichtigte Wirkung hinsichtlich der tatsächlichen Verbesserung der Informationssicherheit nur beschränkt entfaltet (vgl. auch Prüfziele 5 und 14).

Prüfziel 14	Prüfen, ob • die Ressourcen, Rollen oder Kompetenzen zur Umsetzung des konzipierten ISMS vorhanden und plausibel adressiert sind;

	• kein erkennbarer Gap zwischen Konzeptgestaltung und realistischer Umsetzbarkeit des konzipierten ISMS besteht.
Status	**Feststellungen und Einschätzung IR SECO**
🟡	<u>Verbesserungspotenzial (Nettorisiken)</u> Die Anforderungen an die Informationssicherheit wurden definiert und im ISMS-Konzept sowie in den dazugehörenden Dokumenten verankert. Die operative Umsetzung der Vorgaben liegt bei den Security-Verantwortlichen der einzelnen Bereiche sowie bei den ISDS-Verantwortlichen der Systeme und IT-Projekte im SECO. Diese Rollen müssen im Rahmen des ISMS noch klar zugewiesen und entsprechend geschult werden. Aufgrund der detaillierten und umfangreichen Vorgaben kann nicht ausgeschlossen werden, dass bei den Mitarbeitenden, welche deren Umsetzung sicherstellen sollen, Widerstände entstehen. In diesem Zusammenhang kommt den Rollen der 2nd Line (taktische Ebene bei der Sicherheitsorganisation), insbesondere ISBO, ISO und IT-Risk-Manager, eine zentrale Bedeutung zu. Sie müssen die Einhaltung der Vorgaben wirksam überwachen und sicherstellen, beispielsweise durch stichprobenweise Prüfungen, die Überwachung von KPIs, das Einfordern von Evidenzen, das Hinterfragen von Risiken, ein angemessenes Reporting sowie Eskalationen. Die Wirksamkeit des ISMS basiert zudem wesentlich auf einem kontinuierlichen Verbesserungsprozess im Sinne des PDCA-Zyklus (vgl. Prüfziel 5). Aus unserer Sicht ist derzeit fraglich, ob die hierfür erforderlichen Kontrolltätigkeiten und kontinuierlichen Verbesserungsprozesse mit den aktuell verfügbaren Ressourcen angemessen sichergestellt werden können. Siehe **Empfehlung 2**.

Prüfziel 15	Prüfen, ob der Kosten-Nutzen-Aspekt berücksichtigt ist.
Status	**Feststellungen und Einschätzung IR SECO**
🟢	Die gesetzlichen Anforderungen an ein ISMS sind in der ISV klar formuliert und orientieren sich stark an der ISO/IEC 27001. Die ISO-Norm ist anspruchsvoll, jedoch international anerkannt und bietet bei einer korrekten Umsetzung eine systematische Grundlage zur Gewährleistung der Informationssicherheit innerhalb einer Organisation. Dabei ist wesentlich, dass nicht nur klare Vorgaben und Prozesse definiert und die Mitarbeitenden entsprechend geschult werden (wie aktuell im Rahmen der Einführungsphase im SECO), sondern auch ein zweckmässiger kontinuierlicher Verbesserungsprozess (KVP) sichergestellt wird. Gerade der KVP ermöglicht es, das vorgesehene ISMS laufend

	zu optimieren und an organisatorische sowie operative Entwicklungen anzupassen. Wie bereits in den vorangehenden Punkten festgestellt, haben wir Vorbehalte hinsichtlich der ausreichenden personellen Ressourcen, um einen wirksamen KVP sicherzustellen. Aus unserer Sicht ist die Entscheidung der beiden ISBO, ein ISMS auf Basis der ISO 27001 einzuführen, grundsätzlich nachvollziehbar und zweckmässig. Dieser Ansatz stellt wahrscheinlich die einfachste Möglichkeit dar, ein systematisches ISMS aufzubauen, das sich an einem etablierten Industriestandard orientiert. Ohne einen solchen standardisierten Ansatz hätte das Risiko bestanden, dass wesentliche Elemente der Informationssicherheit nicht oder nur unvollständig berücksichtigt worden wären. Eine punktuelle Analyse der Unterschiede zwischen den Minimalanforderungen gemäss ISV und den Anforderungen des ISO-Standards unter Berücksichtigung der spezifischen Gegebenheiten im SECO hätte aus unserer Sicht einen erheblichen zusätzlichen Analyse- und Abstimmungsaufwand verursacht. Wir beurteilen das gewählte Vorgehen daher insgesamt als pragmatisch und zielführend. Gleichzeitig bietet es die höchste Wahrscheinlichkeit, die Konformität mit den gesetzlichen Anforderungen (bzw. mit dem ISO-Standard) langfristig und nachhaltig sicherzustellen.

Anhang 1: Empfehlungsübersicht mit den Stellungnahmen

#	Empfehlung	Priorität	Stellungnahme / Massnahme	Verantwortung[7]	Termin
1	Wir empfehlen den ISBOs, die Liste der Verbesserungsvorschläge im Anhang 2 zu berücksichtigen und die erwähnten Aspekte im Rahmen der laufenden Einführung des ISMS umzusetzen.	Mittel	Die Überprüfung wird durch die InfoSec Organisation sehr geschätzt. Die Empfehlungen und Verbesserungsvorschläge im Anhang 2 werden bis zur Einführung am 01.01.2027 des ISMS ergänzt und wo fehlend, noch implementiert.	ISBO SECO «classico» ISBO TC	31.12.2026
2	Wir empfehlen dem ISVV des SECO, die Situation im Verlauf der zweiten Jahreshälfte 2026 sowie im Jahr 2027 eng zu beobachten und bei Bedarf eine Aufstockung der Ressourcen zur Gewährleistung der Kontrollfunktionen im Bereich des ISMS zu beurteilen.	Mittel	Die Überprüfung wird durch die InfoSec Organisation sehr geschätzt. Die Empfehlung wird umgesetzt.	ISVV	31.12.2027

Übergeordnete Stellungnahme der InfoSec Organisation

Wir bestätigen hiermit unser Einverständnis mit dem Audit, seinen fachlichen Aussagen und den sich daraus ergebenden Massnahmen. Die Arbeiten schreiten gut voran und wir werden sehr gerne die wertvollen Inputs einfliessen lassen.

Schlussbeurteilung DBIR zu den Stellungnahmen

Wir sind mit den vorgeschlagenen Massnahmen einverstanden.

[7] Verantwortlichkeit zur Umsetzung der Empfehlung.

Anhang 2: Verbesserungsvorschläge im Zusammenhang mit Empfehlung 1

Verbesserungsvorschläge	Check	Prüfziel
1. ISMS-Aufgaben in den Stellenbeschreibungen der betroffenen Mitarbeitenden integrieren.	☐	**1**
2. Rollen und Verantwortlichkeiten im Bereich «*Operative Sicherheit*»[8] den zuständigen Mitarbeitenden zuweisen.	☐	
3. Zusammensetzung des Steuerungsgremiums «*IT-Security Board*» definieren und dokumentieren.	☐	
4. Berichterstattung zu IT-Risiken an Business-Risikomanagement klarer definieren (Inhalt und Periodizität).	☐	**3**
5. Standardisierter Austausch mit dem BCM-Verantwortlichen des SECO im ISMS-Konzept regeln.	☐	
6. Schnittstelle zu ITSCM klarer definieren und im ISMS-Konzept verankern.	☐	
7. Klar operationalisierbare Sicherheitsziele definieren und darauf aufbauend geeignete KPIs festlegen.[9]	☐	**4**
8. Dokumentation zum Changemanagement-Prozess ausarbeiten und im ISMS-Konzept formell verankern.	☐	**7**
9. Vertragsvorlagen erstellen (und im ISMS-Konzept verankern), die abhängig von der Art der bearbeiteten Informationen sämtliche definierten Mindestanforderungen zur Informationssicherheit standardisiert abdecken.	☐	
10. Klare Vorgaben zur Verwaltung, Überprüfung und Aktualisierung der Liste der relevanten gesetzlichen Grundlagen, des Inventars der Schutzobjekte und der Ausnahmeliste definieren und einen entsprechenden Aktualisierungsprozess festlegen.	☐	**10**
11. Schnittstelle zu Krisenmanagement klarer definieren und im ISMS-Konzept verankern.	☐	**12**
12. Vertragliche Verpflichtungen in die Übersicht der relevanten gesetzlichen Grundlagen aufnehmen.[10]	☐	

[8] SEC-V, ISDS-V, Asset-Owner, Risk-Owner.

[9] z. B. könnten die operativen Ziele „*Wir wissen, welche Daten durch uns bearbeitet, werden*“ und „*Wir wissen, wo diese Daten liegen und wem sie gehören*“ zusammengeführt werden. Ein mögliches Ziel wäre: „*Alle geschäftskritischen Daten sind inventarisiert und mit Data Ownern sowie Speicherorten dokumentiert*“. Ein solches Ziel ist besser operationalisierbar und ermöglicht eine messbare Bewertung des Zielerreichungsgrads. Ein möglicher KPI könnte messen, welcher Anteil der inventarisierten geschäftskritischen Daten über einen dokumentierten Data Owner und Speicherort verfügt.

[10] Falls derzeit keine spezifischen vertraglichen Verpflichtungen mit Auswirkungen auf die Informationssicherheit bestehen, sollte dies ausdrücklich festgehalten werden, damit das Fehlen entsprechender Angaben nicht als Lücke interpretiert wird.

13. Anhang zu den Schutzobjekten fertigstellen.	☐	
14. Möglichkeit von Ausnahmen gemäss Art. 9 ISV im ISMS-Konzept erwähnen.	☐	
15. Thema «*Kontrollaufgaben der Vorgesetzten*» in den Schulungen aufnehmen.	☐	
16. Dokument «*Prozessbeschreibung Security Incident Management ISMS*» fertigstellen.	☐	