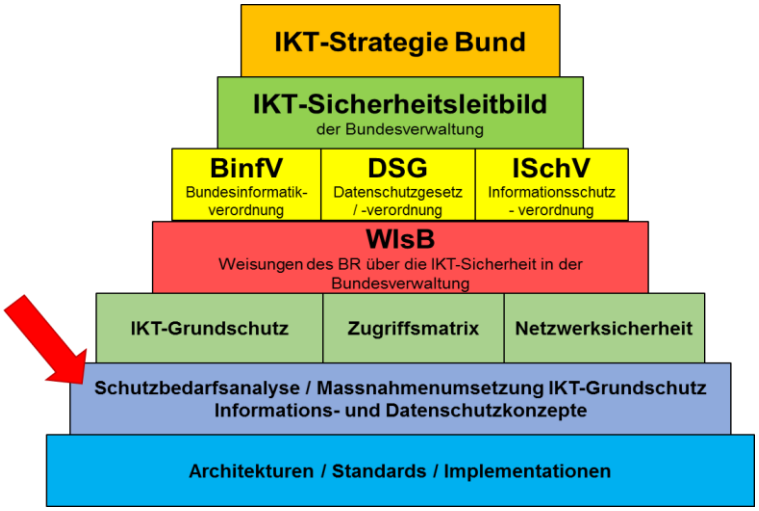
Folgende Arbeitsblätter sind auszufüllen:

Deckblatt:
- Vollständig ausfüllen.
- Ergebnis der Einstufung wird aus den Arbeitsblätter "Einstufung" übernommen.
- Ziel der Farben bei den Feldern der Einstufung ist, deutlich hervorzuheben wo normaler oder erhöhter Schutzbedarf besteht, denn daraus sind die entsprechenden Schutzanforderungen abzuleiten.
  --> Siehe dazu Erklärungen weiter unten

Einstufung:
- Jedes Dropdown-Feld in der Spalte 'Antwort' auswählen.
- Spalte 'Kommentar, Begründung', so ausführlich wie möglich, so gering wie nötig.

Beschreibung:
- Ausführliche Beschreibung des Projektes. bzw. des Schutzobjektes.
- Kommunikationspartner und Datenhaltung ausfüllen.
- Hier ist eine erste Architekturskizze (anstelle des Beispiels) einzufügen. Sie kann allenfalls als eigenständiges Dokument geführt werden. Dann ist in diesem Arbeitsblatt zu vermerken wie das Dokument heisst, welche Version sich auf diese Schutzbedarfsanalyse bezieht und wo es gespeichert ist.



Erhöhter Schutzbedarf:

Erhöhter Schutzbedarf liegt vor, sobald eines der Felder aus der Einstufung im Bereich der Vertraulichkeit als rot gekennzeichnet wird oder wenn mehr als zwei Kriterien in den Bereichen Verfügbarkeit, Integrität oder Nachvollziehbarkeit als rot gekennzeichnet werden. Bei ausgewiesenem, erhöhtem Schutzbedarf ist ein Informationssicherheits- und Datenschutzkonzepts (ISDS-Konzept) zu erarbeiten. Darin sind, neben den Grundschutzmassnahmen, zusätzliche Sicherheitsanforderungen spezifisch für das Projekt und das IKT-Schutzobjekt zu definieren.

Bei erhöhten Anforderungen nur in den Bereichen Verfügbarkeit, Integrität oder Nachvollziehbarkeit (max. zwei Kriterien) müssen zusätzliche Sicherheitsanforderungen als Erweiterung des IKT-Grundschutzes dokumentiert werden. Dies erfolgt vorzugsweise im Dokument «Massnahmenumsetzung des IKT-Grundschutzes», zum Beispiel in Form eines zusätzlichen Kapitels.

Trifft das Kriterium RINA-Relevanz zu, ist der Prüfprozesses RINA (gemäss Anleitung RINA) zu durchlaufen. RINA ist in erster Priorität ein Sensibilisierungsprozess. Er beleuchtet mögliche Bedrohungen betreffend einer nachrichtendienstlichen Ausspähung.

Umsetzung IKT-Grundschutz:

Die Umsetzung der minimalen Sicherheitsvorgaben (IKT-Grundschutz) ist zu dokumentieren (gemäss WIsB Ziffer 3.2, Abs. 3). Dazu steht Ihnen das Word-Dokument «Massnahmenumsetzung zum IKT-Grundschutz in der Bundesverwaltung» auf der Webseite des ISB zur Verfügung. Sie finden es unter der Rubrik IKT-Vorgaben > Sicherheit > Si001 - IKT-Grundschutz in der Bundesverwaltung > Massnahmenumsetzung zum IKT-Grundschutz in der Bundesverwaltung.

Die Gültigkeitsdauer der Schutzbedarfsanalyse beträgt maximal 5 Jahre.

eWertschriften EWS **INTERN**

EWS - Schutzbedarfsanalyse	
Projektname / Schutzobjektname	eWertschriften EWS
Departement	EFD
Amt	ESTV
Projekt Nr. / Projekt ID	keine
Unterstützte Geschäftsprozesse	eWertschriften EWS

Geschäftsprozessverantwortlicher	Dr. Felix Sager, Ressort Logistik/Informatik SSK
Projektleiter (PL LB)	Michael Baeriswyl, Delegierter SSK Ressort Informatik
Informationssicherheits- und Datenschutzverantwortlicher ISDS-V	Dr. Felix Sager, Ressort Logistik/Informatik SSK
Informatiksicherheitsbeauftragter ISBO	Levent Ildeniz, Informationssicherheitsbeauftragter
Dokument ausgefüllt durch	Bruno Buess, Ext. Experte

Ergebnis der Einstufung	
Vertraulichkeit:	*Personendaten*
	Klassifizierung: INTERN
	Erhöhte Anforderungen an die Vertraulichkeit
Verfügbarkeit:	*Ausfalldauer grösser 12 Std.*
	Servicezeiten Standard (11/5)
	ITSCM / BCM nicht notwendig
Integrität:	*Spezielle Anforderungen*
Nachvollziehbarkeit:	*Spezielle Anforderungen*
RINA-Relevanz:	*Nein - Nicht RINA-relevant*

Änderungskontrolle		
Version	**Datum**	**Name / Bemerkungen**
0.1	19.06.2020	Bruno Buess, Initialversion zum Rev. PL/ISBO
0.2	17.08.2020	Bruno Buess, Einpflegen Review-Befunde ISBO
0.3	30.09.2020	Bruno Buess, Einpflegen Review-Befunde
1.0	28.12.2020	Bruno Buess, Abnahme Atamira PA am 15.10.2020
1.1	29.11.2021	Bruno Buess, Ergänzung Aktionärsregistrierung (ohne Name), Nachvollziehbarkeit und Namen bei Unterschriften

Die Gültigkeit dieses Dokuments beträgt maximal 5 Jahre

Unterschriften	**Datum / Name / Unterschrift**
Geprüft: ISBO	Levent Ildeniz, ESTV
Genehmigt: Auftraggeber	Dr. Felix Sager, Ressort Logistik/Informatik SSK
Genehmigt: Geschäftsprozessverantwortlicher	Dr. Felix Sager, Ressort Logistik/Informatik SSK

eWertschriften EWS **INTERN**

Genehmigt: **Projektleiter (PL LB)**	Michael Baeriswyl, Delegierter SSK Ressort Informatik
weitere Unterschriften	

eWertschriften EWS

INTERN

Kriterien	Fragen	Antworten *(Drop Down Felder)*	Kommentare, Begründungen für alle Zeilen ausfüllen
Vertraulichkeit	Sollen [mit diesem Schutzobjekt] Personendaten nach der Datenschutzgesetzgebung bearbeitet werden? Wenn ja, welche Art von Personendaten sind betroffen?	Personendaten	*Die Aktionärsregistrierung erfolgt in EWS. Als Aktionärs-ID wird die AHVN13 verwendet und dazu auch Ort und Land gespeichert.*
	Sollen [mit diesem Schutzobjekt] klassifizierte Informationen nach der Informationsschutzverordnung (ISchV) bearbeitet werden? Wenn ja, Informationen aus welchen Klassifizierungsstufen (vgl. Art. 5 bis 7 ISchV) sind betroffen?	Klassifizierung: INTERN	*Über die Web-Services können Anfragen inkl. Anhänge der kantonalen Steuerbehörden an die ESTV übertragen werden. Die Mitarbeiter der kantonalen Steuerbehörden sind darüber informiert, dass keine sensiblen Daten (ungeschwärzte Printscreens) an die ESTV übertragen werden dürfen. Es liegt also in der Verantwortung der Anwender, dass keine sensiblen Daten an die ESTV übermittelt werden.* *Für die regelmässige DMP-Lieferung an die Lieferantin GFT, werden potentiell sensible Daten beim Export anoymisiert bzw. gelöscht. Dieses Verfahren ist mit dem Datenschutzbeauftragten der ESTV abgestimmt.* *Beim Transport dieser Daten über Web-Services ist die Kommunikation verschlüsselt und kann der Nachrichteninhalt verschlüsselt werden.* *Bis Ende 2021 werden die folgenden Erweiterungen realisiert:* *- Speicherung von Wertschriftenverzeichnissen mit der Angabe einer Dossier-Nummer.* *- Manuelle Auskunft für die Abfrage von NKT und KT Steuerwerten und prüfen der Wertschriftenverzeichnisse* *- Stellen und Verwalten von von Bewertungsaufträgen für BVTax. Statusänderungen werden via BVTax erfasst und vie EWS an die Auftraggeber mitgeteilt.* *- Aktionärsregistrierung für Immobilliengesellschaften. Als Aktionärs-ID wird die AHVN13 verwendet und dazu auch Ort und Land gespeichert.* *Alle Daten können nur in der eigenen (kantonalen) Domäne abgefragt werden.*
	Sollen [mit diesem Schutzobjekt] Informationen oder Daten bearbeitet werden, die aus einem sonstigen Grund (spezielle Gesetzgebungen) besonders geschützt werden müssen? Wenn ja, wie hoch sind die Schutzanforderungen?	Erhöhte Anforderungen an die Vertraulichkeit	*Es werden Daten verarbeitet die Amts- und Steuergeheimnisse darstellen (Art. 320 StGB)*
Verfügbarkeit	Max. zulässige Ausfalldauer?	Ausfalldauer max. 2 Std.	*Abzuklären: Ist mit dem BIT (SLA) für die EWS-Erweiterung zu vereinbaren*
	Servicezeiten?	Servicezeiten 24/7	*Heute gilt für EWS:* *Servicezeiten: 7x24* *Ausfalldauer: 2 h* *Reaktionszeit:* *- Telefon: 15 Minuten* *- Mail und Webtickets: 30 Minuten* *Interventionszeit:* *- Geschäftskritisch: 1 Stunde* *- Mittel: 4 Stunden* *- Standard: 8 Stunden*

eWertschriften EWS

INTERN

Kriterien	Fragen	Antworten *(Drop Down Felder)*	Kommentare, Begründungen für alle Zeilen ausfüllen
	IT Service Continuity Management (ITSCM) relevant [für dieses Schutzobjekt] als Teil des Business Continuity Management (BCM) für geschäftskritische Prozesse?	ITSCM / BCM nicht notwendig	
Integrität	Muss die Echtheit, Korrektheit und/oder Unversehrtheit der Daten nachgewiesen werden können?	Spezielle Anforderungen	*Alle Daten müssen korrekt und nachvollziehbar sein.*
Nachvollziehbarkeit	Müssen bestimmte Arbeitsvorgänge nachgewiesen werden können?	Spezielle Anforderungen	*Die Nachvollziehbarkeit muss sowohl technisch (z.B. Protokollierung der Logins) als auch fachlich (z.B. Protokollierung aller Datenmutationen oder Zugriffe auf schützenswerte Daten) gesichert sein.*
RINA-Relevanz	Ist dieses Schutzobjekt durch nachrichtendienstliche Ausspähung (oder ähnliche) erheblich gefährdet und/oder werden dafür sensitive Beschaffungen notwendig?	Nein - Nicht RINA-relevant	

eWertschriften EWS **INTERN**

Hinweis: Vor der Beantwortung der 5 Fragen ist die Anleitung RINA Kap. 2 zu konsultieren.

Fragen	Antworten	Kommentar / Begründung für alle Kriterien ausfüllen
Kriterium 1 RINA-Relevanz		
Hat das IKT-Schutzobjekt Interdependenzen mit anderen IKT-Infrastrukturen?	nein	EWS hat einen Datenaustausch mit ICTax, mit BVTax und mit kantonalen Systemen. Mittels Mutationsmitteilungen werden veränderte Daten von BVTax an EWS/ICTax für die manuelle Verarbeitung durch die ESTV übermittelt.
Kriterium 2 RINA-Relevanz		
Kann das IKT-Schutzobjekt (gemäss Anleitung RINA, Kap. 2.1) einer der 5 risikorelevanten Kategorien a-e zugeordnet werden?	nein	Remote Wartung oder Support geschieht durch externe von GFT Schweiz AG. Sie haben aber keinen generellen Zugang zu allen Daten sondern im Fehlerfall nur zu Einzeldaten.
Kriterium 3 RINA-Relevanz		
Ist das IKT-Schutzobjekt eine militärisch klassifizierte Beschaffung oder ein militärisch klassifiziertes Schutzobjekt (z.B. Kommunikationsgeräte)	nein	Kein militärisches Schutzobjekt
Kriterium 4 RINA-Relevanz (**bei erhöhtem Schutzbedarf**)		
Erreicht das IKT-Schutzobjekt auf dem folgenden Hilfsblatt Kriterium 5 einen höheren Wert als 61?	Nein	vergl. Hilfsblatt
Müssen Sie den zweiten Schritt des Prüfprozesses RINA durchlaufen	NEIN	

RINA = Risikomanagementmethode zur Reduktion nachrichtendienstlicher Aus

Es müssen zumindest die Felder "Wahrscheinlichkeit und allgemeine Risikobetrachtung" ausgefüllt werden. Wird der Wert 61 überschritten, ist von einer Risikorelevanz gemäss RINA auszugehen und der zweite Schritt RINA gemäss Anleitung durchzuführen. In diesem Fall wird empfohlen, vorab die allgemeine Risikobetrachtung für Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit weiter zu differenzieren.

Ab hier: optional

		Bedrohung Gefährdung	Allgemeine Risikobetrachtung			Begründung für alle Gefahren ausfüllen	Vertraulichkeit		Verfügbarkeit		Integrität		Nachvollziehbarkeit		Kommentar / Begründung (Schwachstellen / Bedrohungen)	Risikokennziffer
			Wahrschein-lichkeit 1 - 5*	Schadens-Ausmass 1 - 4	Risiko Kategorie W(W=B*V)*S=R		Schadens-Ausmass 1 - 4	Risiko Kategorie A*W=R	Schadens-Ausmass 1 - 4	Risiko Kategorie A*W=R	Schadens-Ausmass 1 - 4	Risiko Kategorie A*W=R	Schadens-Ausmass 1 - 4	Risiko Kategorie A*W=R		
G1	Organisatorisch e Mängel	Unbefugter oder schlecht geschützter Zutritt	4	1	4		2	8	2	8	2	8	2	8		32
G2	Vorsätzliche Handlungen	Abhören, Auswerten, Analysen, Hacken, Spoofing	2	1	2	Übertragung erfolgt verschlüsselt	2	4	2	4	2	4	2	4		16
G3		Bösartige Software, Trojaner und Viren	2	1	2	nur durch GFT oder BIT möglich	2	4	2	4	2	4	2	4		16
G4		Gefälschte Daten Integritäts- und Vertraulichkeitsverlust	2	1	2	nur durch interne Mitarbeitende möglic	2	4	2	4	2	4	2	4		16
G5		Manipulieren, kompromittieren, vortäuschen	2	1	2	nur durch interne Mitarbeitende möglic	2	4	2	4	2	4	2	4		16
G6		Missbrauchen von Konten, Zutritten, Berechtigungen usw., Erpressen von Mitarbeitern	3	2	6	nur durch interne Mitarbeitende möglic	2	6	2	6	2	6	2	6		24
G7		Schwachstellen ausnutzen	3	1	3		2	6	2	6	2	6	2	6		24
G8		Unberechtigte Handlungen, Diebstahl (auch z.B. def. HD), Betrug	3	3	9	Die Reports enthalten immer nur Teile	2	6	2	6	2	6	2	6		24
G9		Vandalismus, Anschläge, Sabotagen	2	1	2		2	4	2	4	2	4	2	4		16
	Ergebnis				32											**184**

***Einschätzung soll die entsprechenden Grundschutzmassnahmen bereits berücksichtigen. Die angegebenen Zahlen sind empfohlene Richtwerte und situativ zu überprüfen.**
Falls diese nach unten korrigiert werden, müssen die Werte begründet werden. Die Wahrscheinlichkeit ist die Multiplikation der Bedrohung (Existenz von Akteuren, deren technisch Möglichkeiten und Ressourcen) mal die Verwundbarkeit des Schutzobjekts (R=V*B*S) .
R = Risiko, V = Verwundbarkeit, B = Bedrohung, S = Schadensausmass

Fazit:

Eintretenswahrscheinlichkeit

Stufe	Bemerkung	Beschreibung
1	**Unwahrscheinlich**	Möglich aber eher unwahrscheinlich. Tritt sehr unwahrscheinlich im Lebenslauf eines Objektes ein. Mehr als alle 10 000 Tage (> 27 Jahre)
2	**Selten**	Tritt selten ein, aber man muss mit Eintritt rechnen. Unwahrscheinlich aber gut möglich im Lebenslauf eines Objektes. Alle 1000 bis 10 000 Tage (3 - 27 Jahre)
3	**Möglich**	Tritt gelegentlich ein. Geschieht mehrmals im Lebenslauf eines Objektes. Alle 100 bis 1000 Tage (1/4 - 3 Jahre)
4	**Wahrscheinlich**	Kommt oft vor. Geschieht manchmal im Lebenslauf eines Objektes. Alle 10 bis 100 Tage
5	**sehr wahrscheinlich**	Kommt laufend vor. Geschieht oft im Lebenslauf eines Objekts. Häufiger als alle 10 Tage

Schadensausmass

Stufe	Auswirkung	Beurteilungskriterien
1	**Vernachlässigbar**	Finanzieller Schaden kleiner als 10'000 CHF Die Einhaltung gesetzlicher und vertraglicher Pflichten ist nicht gefährdet Die Aufgabenerfüllung wird höchstens geringfügig beeinträchtigt Persönlichkeitsrechte sind nicht gefährdet Umweltschäden sind minimal Unfälle oder Krankheiten ohne Arbeitsabwesenheiten Kein Imageschaden für die BVerw
2	**Marginal**	Finanzieller Schaden zwischen 10'000 und 200'000 CHF Die Einhaltung gesetzlicher und vertraglicher Pflichten ist gefährdet oder die Erfüllung wesentlicher Aufgaben ist beeinträchtigt Persönlichkeitsrechte sind gefährdet Umweltschäden, welche wieder gut gemacht werden können Unfälle oder Krankheiten mit mehreren verlorenen Arbeitstagen aber ohne bleibende Schäden sind möglich Imageschaden für die BVerw ist klein und von kurzer Dauer (kein Fernsehen und höchstens Kurzmeldung in der Presse)
3	**Kritisch**	Finanzieller Schaden zwischen 200'000 und 1`000'000 CHF Die Einhaltung gesetzlicher und vertraglicher Pflichten stark eingeschränkt oder die Erfüllung wesentlicher Aufgaben verunmöglicht Persönlichkeitsrechte sind in hohem Masse gefährdet Umweltschäden, welche wieder gut gemacht werden können Unfälle oder Krankheiten mit Hospitalisierung und bleibenden Schäden (Teil-Invalidität) Grösserer Imageschaden für die BVerw (Artikel in Presse, aber nicht Seite 1 - kein Fernsehen)
4	**Katastrophal**	Finanzieller Schaden > 1'000'000 CHF Einhaltung gesetzlicher und vertraglicher Pflichten bzw. die Erfüllung wesentlicher Aufgaben verunmöglicht Verletzung der Persönlichkeitsrechte Leib und Leben sind gefährdet Bleibende Umweltschäden entstehen Grosser Imageschaden für BVerw (Seite 1-Meldung in Presse und Fernsehen)

eWertschriften EWS **INTERN**

Anleitung zur Reduktion des Risikos der Amtsgeheimnisverletzung

Aufgrund des Art. 320 StGB ist zu überprüfen, ob beim vorliegenden IKT-Schutzobjekt Amtsgeheimnisse (Privat- und Dienstgeheimnisse) verarbeitet werden und das Risiko besteht, dass die Daten bei der Inbetriebnahme, Wartung, Support etc. auswärtigen Dritten offenbart werden müssen.
Folgend Grundlagen sind dazu zu konsultieren:

- Massnahme 15.2.1 IKT-Grundschutz
- Dokument «Anforderungen angesichts des Risikos von Amtsgeheimnisverletzungen in der Bundesverwaltung»
- Entsprechende Richtlinien des Departements zum Einwilligungsprozess der Inhaber der Daten bzw. der vorgesetzten Behörde.

Schritt 1: Werden Daten bzw. Informationen verarbeitet, die Amtsgeheimnisse darstellen?
Wenn "Nein" Prozess abgeschlossen; Wenn "Ja" weiter zu Schritt 2. ja

Schritt 2: Ist davon auszugehen, dass während des Life Cycles des Schutzobjektes externe IKT-Fachkräfte Zugang zu diesen Daten bzw. Informationen erhalten?
Wenn "Nein" Prozess abgeschlossen. Wenn "Ja" weiter zu Schritt 3. ja

Schritt 3: Handelt es sich dabei um Dienst-, Privatgeheimnisse- oder um beide Arten? Im Zweifelsfall ist unbedingt der LB bzw. die entsprechende Rechtsabteilung zu konsultieren.
Weiter zu Schritt 4, wenn nur Dienstgeheimnisse verarbeitet werden. Ansonsten weiter zu Schritt 5. Dienstgeheimnis

Schritt 4: Die Ziffern 15.1.1 und 15.2.1 des IKT Grundschutzes sind so weitgehend wie möglich umzusetzen. Die entsprechende Einwilligung der vorgesetzten Behörde ist gemäss den amts- bzw. departementsspezifischen Prozessen einzuholen.
Prozess abgeschlossen

Schritt 5: Die Ziffer 15.2.1 des IKT Grundschutzes sind so weitgehend wie möglich umzusetzen. Die entsprechende Einwilligung der vorgesetzten Behörde und nach Möglichkeit der Datenherren ist gemäss den amts- bzw. departementsspezifischen Prozessen einzuholen. Die verantwortliche Linie (LE und LB) ist ausdrücklich bezüglich des Risikos der Amtsgeheimnisverletzung aufgrund von Privatgeheimnissen zu informieren.
Prozess abgeschlossen.

eWertschriften EWS **INTERN**

Beschreibung des Projektes bzw. Schutzobjektes
Die Applikation EWS ermöglicht den kantonalen Steuerämtern die Veranlagung von Wertschriftenerträgen und Vermögen. Hierzu werden Services zur Suche und Berechnung von Titeln sowie zur suche nach Devisenkursen zur Verfügung gestellt, die in (kantonalen) Drittapplikationen genutzt werden können. ICTax stellt die Daten zu NKT und KT Titeln und Gesellschaften zur Verfügung. Der Steuerzahler, die Kantone und Dritte (zum Beispiel Finanzinstitute) haben die Möglichkeit, via ICTax die Steuerfaktoren zu einzelnen kotierten Wertschriften abzufragen. Mit EWS werden Webservices angeboten, mit denen es möglich ist, ganze Wertschriftenverzeichnisse abzufragen und einzelne Titel berechnen zu lassen. eWertschriften ist die Grundlage für eine "teilautomatisierte" Prüfung und Veranlagung von Wertschriftenerträgen. EWS liegt in der Verantwortung der SSK und ist zusammen mit BVTax Teil des EWV-Systemverbundes. Bis Ende 2021 werden die folgenden Erweiterungen realisiert: - Speicherung von Wertschriftenverzeichnissen mit der Angabe einer Dossier-Nummer. - Manuelle Auskunft für die Abfrage von NKT und KT Steuerwerten und prüfen der Wertschriftenverzeichnisse - Stellen und Verwalten von Bewertungsaufträgen für BVTax. Statusänderungen werden via BVTax erfasst und via EWS an die Auftraggeber mitgeteilt. - Aktionärsregistrierung für Immobiliengesellschaften und Bewertungsaufträge. Als Aktionärs-ID wird die AHVN13 verwendet, wobei auch Ort und Land hinterlegt sind. Für die Kantone die heute die Auskunft von WVK einsetzen wird in EWS eine Minimallösung für die manuelle Auskunft zu NKT und KT Titeln zur Verfügung gestellt. Die Webservice Benutzerzugriffe auf EWS erfolgen über das Web-Service-Gatewav (WSG) mittels Klasse C-Zertifikate. Sämtliche Benutzerzugriffe auf EWS für die manuelle Auskunft erfolgen über eIAM (Identitätsmanagement-System) des BIT. eIAM führt die Authentisierung der Benutzer durch und vergibt eine Auto-Grant-Rolle für den Applikationszugriff. Die Rollen, die Berechtigungen innerhalb des Systems steuern, werden in EWS direkt verwaltet. Die Nachvollziehbarkeit wird sowohl technisch (z.B. Protokollierung der Logins) als auch fachlich (z.B. Protokollierung aller Datenmutationen oder Zugriffe auf schützenswerte Daten) sichergestellt. Der EWS-Datenaustausch erfolgt mit den folgenden Systemen: - Mit ICTax für ausländische kotierte Titel und Gesellschaften und für nicht kotierte Titel und Gesellschaften (Schnittstelle von ICTax zu ZEFIX und Core-IT). - Mit BVTax für die Bewertungsaufträge. EWS wird durch das BIT betrieben und die Technologien beruhen im wesentlichen auf den Vorgaben des BIT.

Kommunikationspartner und Datenhaltung			
Kommunikationspartner (netzwerktechnisch)	Zugriffe intern BV?	Ja	*Wenn Antwort «Nein» ist zu prüfen inwieweit das System überhaupt im Bundesnetz betrieben werden muss.*
	Zugriffe extern (Internet)?	Nein	*Wenn Antwort «Ja», ist die Art und Weise des Zugriffs gemäss Zugriffsmatrix zu prüfen.*
Datenhaltung	intern BV?	Ja	*Keine über den IKT-Grundschutz hinausgehende Anforderungen.*
	extern (Internet)?	Nein	*Wenn Antwort «Ja», ist zu prüfen ob eine Datenhaltung ausserhalb der BV überhaupt erlaubt ist. Sollte es sich um eine Cloud-Lösung handeln, sind die Sicherheitsempfehlungen zum Cloud Computing des ISB zu prüfen.*

Architekturskizze