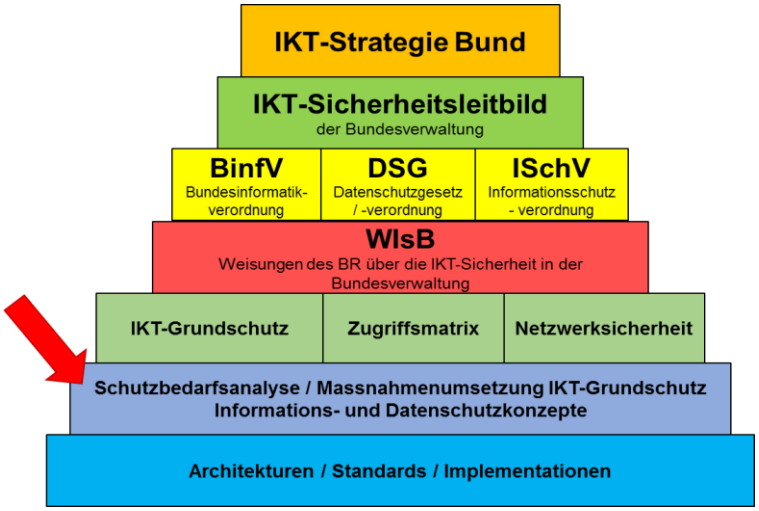
Folgende Arbeitsblätter sind auszufüllen:

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.

BVTax (Business Valuation Tax) **INTERN**

BVTax - Schutzbedarfsanalyse	
Projektname / Schutzobjektname	BVTax (Business Valuation Tax)
Departement	EFD
Amt	ESTV
Projekt Nr. / Projekt ID	keine
Unterstützte Geschäftsprozesse	Wertschriftenbewertung

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:	*Keine 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	26.05.2020	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	17.06.2021	Bruno Buess, Ergänzung 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

BVTax (Business Valuation Tax) **INTERN**

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

BVTax (Business Valuation Tax)

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?	Keine Personendaten	*Die Aktionärsregistrierung erfolgt in EWS. Als Aktionärs-ID wird anstelle des Namens neu die AHVN13 verwendet. Aus BVTax besteht für die Bewerter kein direkter Zugriff auf die Aktionärsregistrierung in EWS.*
	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	*Als INTERN werden Informationen klassifiziert:* *a. deren Kenntnisnahme durch Unberechtigte den Landesinteressen einen Nachteil zufügen kann; und* *b. die weder als GEHEIM noch als VERTRAULICH klassifiziert werden müssen*
	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 grösser 12 Std.	*Abzuklären: Ist mit dem BIT (SLA) zu vereinbaren*
	Servicezeiten?	Servicezeiten Standard (11/5)	*Servicezeiten wie bei WVK*
	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	*Die Berechnung der Steuerwerte und Erträge für nicht-kotierte Aktien müssen für alle Steuerpflichtigen 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) 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	*Vgl. Blatt Einstufung Teil 2 (RINA)*

Weiter mit Einstufung Teil 2 (RINA)

BVTax (Business Valuation Tax) **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	BVTax hat einen Datenaustausch mit EWS und mit kantonalen Systemen. Mittels Mutationsmitteilungen werden veränderte Daten von BVTax an EWS/ICTax für die manuelle Verarbeitung durch die ESTV übermittelt. Die kantonalen Systeme liefern Daten für die Bewertung der nicht-kotierten Unternehmen (JP-/GRUDA-Daten).
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 emineo 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

BVTax (Business Valuation Tax) INTERN INTERN

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	Wahrschein-lichkeit 1 - 5*	Allgemeine Risikobetrachtung		Begründung für alle Gefahren ausfüllen	Vertraulichkeit		Verfügbarkeit		Integrität		Nachvollziehbarkeit		Kommentar / Begründung (Schwachstellen / Bedrohungen)	Risikokennziffer
			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		
Organisatorisch e Mängel	Unbefugter oder schlecht geschützter Zutritt	4	1	4		2	8	2	8	2	8	2	8		32
Vorsätzliche Handlungen	Abhören, Auswerten, Analysen, Hacken, Spoofing	2	1	2	Übertragung erfolgt verschlüsselt	2	4	2	4	2	4	2	4		16
	Bösartige Software, Trojaner und Viren	2	1	2	nur durch emineo oder BIT möglich	2	4	2	4	2	4	2	4		16
	Gefälschte Daten Integritäts- und Vertraulichkeitsverlust	2	1	2	nur durch interne Mitarbeitende möglic	2	4	2	4	2	4	2	4		16
	Manipulieren, kompromittieren, vortäuschen	2	1	2	nur durch interne Mitarbeitende möglic	2	4	2	4	2	4	2	4		16
	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
	Schwachstellen ausnutzen	3	1	3		2	6	2	6	2	6	2	6		24
	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
	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

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)

BVTax (Business Valuation Tax) **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. Dienstgeheim

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.

BVTax (Business Valuation Tax) **INTERN**

Beschreibung des Projektes bzw. Schutzobjektes
Das System BVTax (Business Valuation Tax) ermöglicht den Kantonen die Bewertung von nicht-kotierten Titeln (NKT). Mit rund 820‘000 Gesellschaften, 3.5 Mio. Titeln und jährlich 300‘000 Bewertungen nimmt die BVTax einen wichtigen Stellenwert in der schweizerischen Steuerlandschaft ein. Gegen 200 Bewerter in den 26 Kantonen arbeiten täglich aktiv mit diesem System. Das System BVTax liegt in der Verantwortung der SSK und ist zusammen mit EWS Teil des EWV-Systemverbundes. BVTax ist eine browserbasierte Web-Anwendung und läuft auf den kantonalen Desktop-Systemen. Sämtliche Funktionalitäten sind im Browser ausführbar. Sämtliche Benutzerzugriffe auf BVTax 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 BVTax direkt verwaltet. Die Nachvollziehbarkeit wird sowohl technisch (z.B. Protokollierung der Logins) als auch fachlich (z.B. Protokollierung aller Datenmutationen) sichergestellt. Der Datenaustausch mit BVTax erfolgt mit den folgenden Systemen: - Für nicht kotierte Titel und Gesellschaften und für inländische und ausländische kotierte Titel und Gesellschaften mit EWS (Daten von ICTax und Core-IT (ESTV)). - Über EWS (SSK-System) werden die Bewertungsaufträge an BVTax gestellt, ebenso erfolgt die Aktionärsregistrierung in EWS. EWS stellt auch die manuelle Auskunft für kotierte und nicht-kotierte Titel für die Kantone zur Verfügung. - Über eine SOAP-Schnittstellen erfolgt der Datenaustausch mit den kantonalen Systemen für JP-Veranlagungsdaten und Gründstückdaten sowie für die Archivierung der Eröffnungsschreiben. BVTax wird durch das BIT betrieben und die Technologien beruhen im wesentlichen auf den Vorgaben des BIT. Daneben werden verschieden OpenSorce und proprietäre Technologien eingesetzt. Die Details sind aus dem Dokument "BVTAX Systemarchitektur-v21-20200520_112736" ersichtlich.

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