Schweizerische Steuerkonferenz
Conférence suisse des impôts
Conferenza svizzera delle imposte

**Wenn ausgefüllt mindestens: INTERN**

# Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept)

## BVTax (Business Valuation Tax)

---

| | |
|---|---|
| **Klassifizierung** | **INTERN** / VERTRAULICH / GEHEIM |
| **Status** | in Arbeit / in Prüfung / **genehmigt zur Nutzung** |
| **Projektnummer** | |
| **Projektleiter** | Michael Baeriswyl |
| **Version** | V1.5 |
| **Datum** | 08.11.2024 |
| **Auftraggeber** | Schweizerische Steuerkonferenz SSK |
| **Autor/Autoren** | Bruno Buess |

## Änderungskontrolle

| Version | Datum | Beschreibung, Bemerkung | Name |
|---|---|---|---|
| **0.1** | 03.08.2020 | Initialversion | Bruno Buess |
| **0.2** | 17.08.2020 | Einpflegen Review-Befunde ISBO | Bruno Buess |
| **0.3** | 30.09.2020 | Einpflegen Review-Befunde | Bruno Buess |
| **0.4** | 05.10.2020 | Nachtrag Korrektur Kap. 2.3 | Bruno Buess |
| **1.0** | 28.12.2020 | Abnahme Atamira PA - 15.10.2020 | Bruno Buess |
| **1.1** | 17.06.2021 | Korrektur Kap.4, Tabelle.3, Beschreibung Vertraulichkeit | Bruno Buess |
| **1.2** | 09.06.2023 | Anpassung Kap. 4, Weitere Ergänzungen/Korrekturen | Bruno Buess |
| **1.3** | 22.06.2023 | Anpassung Kap. 3 u. Kap. 5.7 | Bruno Buess |
| **1.4** | 28.12.2023 | Aktualisierung Kap. 3 | Bruno Buess |
| **1.5** | 08.11.2024 | Aktualisierung Kap.3 Verzeichnis sicherheitsrelevante Dokumente, Ergänzung Kap.10 Abkürzung | Bruno Buess |

## Verteiler

| Funktion | Name | Departement / Amt |
|---|---|---|
| **ISBO** | Matthias Schwaller | ESTV |
| **ISDS-V** | Felix Sager | Ressort Logistik/Informatik SSK |
| **PL-LB** | Michael Baeriswyl | Delegierter SSK Ressort Informatik |
| | | |
| | | |

**Prüfung des Dokuments nach den Projektphasen**

Die Tabellen mit Personen die die einzelnen Phasen einsehen (bestätigen) können beliebig ergänzt werden.

Initialisierung – vor Projektfreigabe

| Version | Funktion | Name | Datum |
|---|---|---|---|
| | ISDS-V | Felix Sager | |
| | ISBO | Matthias Schwaller | |
| | PL-LB | Michael Baeriswyl | |
| | | | |

Konzept – vor Phasenfreigabe

| Version | Funktion | Name | Datum |
|---|---|---|---|
| | ISDS-V | Felix Sager | |
| | ISBO | Matthias Schwaller | |
| | PL-LB | Michael Baeriswyl | |
| | | | |

Realisierung – vor Phasenfreigabe

| Version | Funktion | Name | Datum |
|---|---|---|---|
| | ISDS-V | Felix Sager | |
| | ISBO | Matthias Schwaller | |
| | PL-LB | Michael Baeriswyl | |
| | | | |

Einführung – vor Betriebsaufnahme

| Version | Funktion | Name | Datum |
|---|---|---|---|
| | ISDS-V | Felix Sager | |
| | ISBO | Matthias Schwaller | |
| | PL-LB | Michael Baeriswyl | |
| | | | |

# Inhaltsverzeichnis


**1 Generelle Anmerkungen ..... 6**

**1.1 Beschreibung ..... 6**
**1.2 Zweck des Dokuments ..... 6**
**1.3 Gültigkeit des Dokuments ..... 6**

**2 Management Summary ..... 7**

**2.1 Allgemeines ..... 7**
**2.2 Zusammenfassung Restrisiken ..... 7**
**2.3 Empfohlene Massnahmen ..... 7**
**2.4 Abschliessende Bemerkungen ..... 9**
**2.5 Genehmigung ..... 10**

**3 Verzeichnis der sicherheitsrelevanten Dokumente ..... 11**

**4 Einstufung Schutzbedarf ..... 12**

**4.1 Risikomanagementmethode zur Reduktion nachrichtendienstlicher Ausspähung (RINA Prüfprozess) ..... 14**
4.1.1 Kriterien ..... 14

**5 Sicherheitsrelevante Systembeschreibung ..... 16**

**5.1 Ansprechpartner / Verantwortlichkeiten ..... 16**
**5.2 Informationssicherheit ..... 16**
**5.3 Beschreibung des Gesamtsystems ..... 17**
**5.4 Beschreibung der zu bearbeitenden Daten ..... 18**
**5.5 Architekturskizze / Systemübersicht ..... 18**
**5.6 Beschreibung der zugrundeliegenden Technik ..... 19**
**5.7 Rollen und Berechtigungen ..... 21**

**6 Risikoanalyse und Schutzmassnahmen ..... 24**

**6.1 Restrisiken ..... 24**
**6.2 Fortlaufende Umsetzung der Schutzmassnahmen ..... 27**
**6.3 Potenzielle sicherheitsrelevante Vorfälle ..... 28**

**7 Wiederherstellung des Geschäftsbetriebes ..... 29**

**8 Einhaltung / Überprüfung / Abnahme der Schutzmassnahmen ..... 29**

**8.1 Allgemeines ..... 29**
**8.2 Aufrechterhaltung der Sicherheitsmassnahmen im laufenden Betrieb ..... 30**
**8.3 Systemabnahmeprüfung ..... 30**
**8.4 Zugriff auf bewirtschaftete Daten ..... 31**
**8.5 Spezifische Kontrollen ..... 31**

**9 Ausserbetriebnahme ..... 31**

**10 Abkürzungen ..... 32**

**11 Anhang ..... 33**

# Abbildungen

Abbildung 1: Systemübersicht BVTax mit Schnittstellen zu Umsystemen ..... 19
Abbildung 2: Datenflüsse bei einer serverseitigen Schnittstelle auf BVTax ..... 21
Abbildung 3: eIAM Authenthisierungsstufen ..... 22
Abbildung 4: BVTax eIAM-Rollen ..... 22
Abbildung 5: Restrisikomatrix aus BVTax-ISDS-Sicherheitsanalyse ..... 24

# Tabellenverzeichnis

Tabelle 1: Empfohlene Massnahmen ..... 9
Tabelle 2: Verzeichnis sicherheitsrelevanter Dokumente ..... 11
Tabelle 3: Erhöhter Schutzbedarf aus der SCHUBAN ..... 13
Tabelle 4: Rollen und Berechtigungen ..... 23
Tabelle 5: Restrisiken aus der Überprüfung der IKT-Grundschutz Umsetzung ..... 25
Tabelle 6: Restrisiken aus der Risikoanalyse ..... 27
Tabelle 7: Massnahmenliste ..... 28
Tabelle 8: Liste der möglichen Sicherheitsrelevanter Vorfälle ..... 29
Tabelle 9: Liste der Prüfungen und Kontrollen ..... 31
Tabelle 10: Anhänge zum ISDS-Konzept ..... 33

# Anhang

BIT BVTax-Architektur

# 1 Generelle Anmerkungen

## 1.1 Beschreibung

Das ISDS-Konzept gilt als Hauptdokument der Informationssicherheit und des Datenschutzes im Projekt und während des Betriebes. Die Einstufung erfolgt gemäss der Schutzbedarfsanalyse nach CyRV.

## 1.2 Zweck des Dokuments

Das ISDS-Konzept legt die nötigen Angaben zur Erhaltung und Verbesserung der Informationssicherheit und des Datenschutzes fest. Es fasst die Aspekte der Informationssicherheit und des Datenschutzes im Projekt zusammen.

Für eine korrekte Grundlage eines IKT-Vorhabens ist die Verordnung über die digitale Transformation und die Informatik ein wesentlicher Bestandteil.

Sämtliche IKT-Vorhaben müssen in aktueller Form dokumentiert werden.
Dazu dient unter anderem dieses ISDS-Konzept.

## 1.3 Gültigkeit des Dokuments

Die Gültigkeit eines ISDS-Konzepts beträgt maximal 5 Jahre.

# 2 Management Summary

## 2.1 Allgemeines

Das vorliegende ISDS-Konzept basiert auf den folgenden Ergebnissen:

1. Der Schutzbedarfsanalyse - Beilage [SCHUBAN]
2. Überprüfung der IKT-Grundschutz Umsetzung - Beilage [GRUNDSCHUTZ]
3. Durchführung der Risikoanalyse mit Massnahmenliste - Beilage [RISIKOANALYSE]

Die Schutzbedarfsanalyse hat gezeigt, dass ein erhöhter Schutzbedarf vorliegt und damit eine Risikoanalyse durchgeführt und das vorliegende ISDS-Konzept erstellt werden muss. Die Überprüfung der IKT-Grundschutz Umsetzung hat eine Reihe von Risiken gezeigt, welchen mit den im Kapitel 2.3 empfohlenen Massnahmen begegnet wird.

## 2.2 Zusammenfassung Restrisiken

Die in der Überprüfung der IKT-Grundschutz Umsetzung und der Risikoanalyse identifizierten Mängel müssen nicht alle behoben werden. Einige davon sind als Restrisiken akzeptierbar. Die Liste dieser in Kauf genommenen Risiken ist im Kapitel Restrisiken aufgeführt.

## 2.3 Empfohlene Massnahmen

Aufgrund der Überprüfung der IKT-Grundschutz Umsetzung [GRUNDSCHUTZ] und der Risikoanalyse [RISIKOANALYSE] schlagen wir die folgenden Sicherheitsmassnahmen vor, über deren Umsetzung der Auftraggeber entscheiden muss:

| Nr. | Sicherheitsanforderung | Vorgeschlagene Massnahme |
|---|---|---|
| | Aus der IKT-Grundschutz Umsetzung | |
| 2.1.1 | Nur Smart Devices, welche über ein Mobile Device Management (MDM) verwaltet werden, dürfen mit Systemen der Bundesverwaltung kommunizieren.<br>Ausgenommen davon sind anonyme und personalisierte Zugriffsmöglichkeiten zu E-Government-Anwendungen oder öffentliche Web-Auftritte der Bundesverwaltung. | Der Einsatz von mobilen Geräten ist für BVTax nicht vorgesehen. Sollte der Einsatz von (privaten) Tablets zugelassen werden, dann erfolgt der Zugang über eIAM mit 2 Faktor Authentisierung via SMS-Code. |
| 7.1.7 | Der Zugriff von Personen auf Arbeitsplatz- und Serversysteme der Bundesverwaltung darf nur über eine 2-Faktor-Authentisierung möglich sein. | Mit der eIAM-Integration wird sichergestellt, dass die Authentifizierung den Vorgaben entspricht. |

| | | |
|---|---|---|
| 9.2 | Die Administration von Serversystemen erfolgt auf einem (logischen) getrennten Administrationsnetz und ist über dedizierte und gesondert abgesicherte IKT-Systeme auszuführen. Dieses Netz darf keinen Zugriff zum Internet und zur Bürokommunikation (i.e. Mailbox) haben. Wenn technisch nicht umsetzbar, muss die Art und Weise des Administrationszugangs in einem ISDS-Konzept beschrieben werden.<br>Für den Zugriff auf diese administrative Managementebene bzw. auf die zu administrierenden Zielsysteme ist eine 2-Faktor-Authentifizierung umzusetzen. | Die BVTax Serversysteme sind nur durch berechtigte Administratoren aus dem BIT erreichbar. Mit der eIAM-Integration wird sichergestellt, dass die Authentifizierung den Vorgaben entspricht. |
| 8.2<br>8.3<br>8.4<br>12.1.3<br>16.1 | Ein Organisationshandbuch muss vor Inbetriebnahme fertiggestellt und freigegeben werden. | Das Organisationshandbuch (OHB) muss für BVTax unter Mitwirkung von LE (BIT und emineo AG) und LB erstellt und vom Auftraggeber freigegeben werden. |
| 7.1.9<br>13.1.7 | Datenzugriffe auf BVTax dürfen nur verschlüsselt erfolgen. Die Daten sind bei der Übertragung zu verschlüsseln.,. | Alle Zugriffe erfolgen verschlüsselt mit HTTPS und SSL/TLS (TLS 1.2)<br>*Hinweis:* Aufgrund einer Sicherheitslücke dürfte das BIT auf TLS 1.3 umstellen |
| 14.2.1 | Testdaten sind entsprechend ihrer Einstufung zu schützen.<br>Ist es unumgänglich, dass produktive Daten zu Testzwecken verwendet werden, sind diese gemäss ihrer Einstufung zu schützen. | Ist durch die LE (BIT und emineo) technisch und organisatorisch sichergestellt.<br>Der Standort der Entwicklungs- und Testumgebung (Server und Datenbanken) in der Schweiz ist sicherzustellen. |
| | Aus der Risikoanalyse: | |
| R1<br>R2 | Ausfallsicherheit erhöhen | Der LE BIT betreibt Rechenzentren an verschiedenen Standorten. Die Datenbackups sind an verschiedenen Orten gespeichert. Damit ist ein Recovery innert nützlicher Frist möglich, wobei dies mit den LE (BIT und emineo) im Rahmen des SLA zu regeln ist. |
| R2 | Ausfallsicherheit erhöhen | Die Systeme (Netze, Power, etc.) sind redundant ausgelegt. Mit entsprechenden Massnahmen (Monitoring, etc.) kann das Risiko vermindert werden. |

| | | |
|---|---|---|
| R4<br>R10 | Zugriffsschutz, Manipulation von Daten | Mit der eIAM-Integration wird sichergestellt, dass nur berechtigte Benutzer Zugang haben und die Authentifizierung den Vorgaben entspricht. |
| R6 | Betriebsmittel sicherstellen | Die Betriebszeiten von 5x11h sind sichergestellt. |
| R6 | Betriebsmittel sicherstellen, betrifft auch die Finanzierung für den längerfristigen Betrieb von BVTax | Die Finanzierung für den Betrieb von BVTax ist für die SSK durch vertragliche Vereinbarungen mit allen Kantonen für einen längerfristigen Zeithorizont sichergestellt |
| Generell | Umsetzung der Massnahmen<br>Sind alle Massnahmen aus der Risikoanalyse des ISDS-Konzeptes umgesetzt? Sind die Restrisiken dem Kunden mitgeteilt worden? | Es ist ein aktives Risikomanagement zu führen. Die Restrisiken sind dem Kunden mitgeteilt worden. Die Massnahmen aus der Risikoanalyse sind noch umzusetzen. |
| | Aus dem ISDS-Konzept | |
| | Datenbearbeitungsreglement | Mit BVTax werden keine Personendaten verarbeitet. Aber ein «abgespecktes» Datenbearbeitungsreglement ist zu erstellen, da verschiedene kantonale Steuerbehörden mit BVTax arbeiten und Schnittstellen zu kantonalen Systemen bestehen. |
| | Anmeldung der Datensammlung beim EDÖB | Da mit BVTax Personendaten bearbeitet werden, muss die Datensammlung beim EDÖB angemeldet werden. |

**Tabelle 1: Empfohlene Massnahmen**

## 2.4 Abschliessende Bemerkungen

Keine

## 2.5 Genehmigung

Mit seiner Unterschrift bestätigt der Informatiksicherheitsbeauftrage (ISBO) das ISDS-Konzept geprüft zu haben. Insbesondere wurde geprüft ob das Dokument vollständig ausgefüllt ist und alle geforderten Massnahmen dokumentiert sind. Die Angaben wurden kritisch hinterfragt, ob sie konsistent sind und im Kontext des IKT-Schutzobjektes stimmen.

Der Auftraggeber und der Geschäftsprozessverantwortlicher genehmigen mit ihrer Unterschrift das ISDS-Konzept.

Das ISDS-Konzept ist in geeigneter Form dem Leistungserbringer zur Kenntnis zu bringen[1].

Bern,

Datum / Name / Unterschrift
**ISBO**: Levent Ildeniz, ESTV

……..…...

Bern,

Datum / Name / Unterschrift
**Auftraggeber**: Dr. Felix Sager,
Ressort Logistik/Informatik SSK

……..…...

Bern,

Datum / Name / Unterschrift
**Geschäftsprozessverantwortlicher**: Dr. Felix Sager,
Ressort Logistik/Informatik SSK

……..…...

Bern,

Datum / Name / Unterschrift
**Projektleiter (PL LB)**:
Michael Baeriswyl,
Delegierter SSK Ressort Informatik

……..…...

**Weitere Unterschriften, zum Beispiel die des Verantwortlichen beim LE, können hinzugefügt werden.**
**Die Unterschriften können auch in elektronischer Form (in einem PDF) angebracht werden.**

[1] WIsB, Ziffer 2.2 Leistungsbezüger und 2.3 Leistungserbringer

# 3 Verzeichnis der sicherheitsrelevanten Dokumente

Beinhaltet die Auflistung aller informationssicherheitsrelevanten Gesetze, Verordnungen, Weisungen, Regelungen, technische Spezifikationen etc..
Sie wurde durch die Departements- und/oder amtseigenen Dokumente ergänzt.

| Dokumententyp | Titel |
|---|---|
| **Gesetz** | SR 235.1 Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) |
| | SR 128 Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) |
| | SR 152.1 Bundesgesetz über die Archivierung (Archivierungsgesetz (BGA) |
| | SR 172.010 Regierungs- und Verwaltungsorganisationsgesetz (RVOG) |
| | SR 642.14 Bundesgesetz über die Harmonisierung der direkten Steuern der Kantone und Gemeinden (StHG) |
| | SR 642.11 Bundesgesetz über die direkte Bundessteuer (DBG) |
| | SR 642.21 Bundesgesetz über die Verrechnungssteuer (VStG) |
| **Verordnung** | SR 172.010.58 Verordnung über die digitale Transformation und die Informatik (VDTI) |
| | SR 120.73 Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) |
| | Verordnung über die Cybersicherheit (Cybersicherheitsverordnung, CSV)[2] |
| | SR 128.1 Verordnung über die Informationssicherheitssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung, ISV) |
| | SR 235.11 Verordnung über den Datenschutz (Datenschutzverordnung, DSV) |
| | SR 172.010.442 Verordnung über die Bearbeitung von Personendaten und Daten juristischer Personen bei der Nutzung der elektronischen Infrastruktur des Bundes (VBNIB) |
| | SR 172.010.59 Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes (IAMV) |
| | SR 172.010.1 Regierungs- und Verwaltungsorganisationsverordnung (RVOV) |
| | SR 172.010.441 Verordnung über die elektronische Geschäftsverwaltung in der Bundesverwaltung (GEVER-Verordnung) |
| | SR 172.215.1 Organisationsverordnung für das Eidgenössische Finanzdepartement (OV-EFD) |
| **Methode** | HERMES - Die schweizerische Projektführungsmethode |
| ***Weitere:*** | Si001 – IT-Grundschutz in der Bundesverwaltung |
| | Integration von Applikationen mit eIAM, Version 3.0 |
| **SCHUBAN** | BVTax-Schutzbedarfsanalyse, Version 1.1 vom 17.06.2021 |
| **GRUNDSCHUTZ** | Überprüfung der IKT-Grundschutz Umsetzung, Version 1.0 vom 28.12.2020 |
| **RISIKO-ANALYSE** | ISDS Konzept, Risikoanalyse, Version 1.0 vom 28.12.2020 |

**Tabelle 2: Verzeichnis sicherheitsrelevanter Dokumente**

[2] Die Verordnung tritt auf 1. Jan. 2025 in Kraft. Der Link auf die CSV in der Fedlex-Publikationsplattform (https://www.fedlex.admin.ch/) ist dann einzufügen, und alle Links in Kap. 3 auf ihre Aktualität zu überprüfen

# 4 Einstufung Schutzbedarf

In der Schutzbedarfsanalyse [SCHUBAN] wurden die folgenden Aspekte mit erhöhtem Schutzbedarf identifiziert:

| Sicherheitsaspekt | Beschreibung |
|---|---|
| **Vertraulichkeit**<br>Erhöhte Anforderungen an die Schutzwürdigkeit (nicht DSG/ISV relevant) | Es werden Daten verarbeitet die Amts- und Steuergeheimnisse darstellen (Art. 320 StGB).<br>Diese sind als INTERN klassifiziert und dürfen nur von der ESTV und den kantonalen Steuerbehörden genutzt werden.<br>Dies betrifft vor allem die Bewertung von nicht kotierten Schweizer Gesellschaften. Bei Beteiligungen an ausländischen nicht-kotierten Gesellschaften werden auch diese bewertet.<br>BVTax erstellt die Steuerwerte in Form der Bewertung. Die produzierten Steuerwerte werden über EWS zu ICTax publiziert. In BVTax werden die Steuerwerte angezeigt bei den Stillen Reserven, in der Wertübersicht und bei Immobiliengesellschaften mit der Aktionärsregistrierung.<br>Ebenfalls werden ausländische nicht-kotierte Gesellschaften, die zur Bewertung benötigt werden (Beteiligungen), im BVTax erfasst und gepflegt (und als Mutationsmitteilung an EWS geliefert).<br>Die Daten zur wirtschaftlichen Handänderung (Pflichtregistrierung der Aktionäre bei Immobiliengesellschaften) werden in BVTax ausgewertet und sind als Report den Kantonen zugänglich (geplante Erweiterung). |
| **Verfügbarkeit**<br>Max. zulässige Ausfalldauer? | Dies ist mit den LE (BIT und emineo AG) im Rahmen des SLA vereinbart. |
| **Integrität**<br>Spezielle Anforderungen | Die Berechnung der Steuerwerte und Erträge für nicht-kotierte Aktien müssen für alle Steuerpflichtigen korrekt und nachvollziehbar sein. |
| | |

| Sicherheitsaspekt | Beschreibung |
|---|---|
| **Nachvollziehbarkeit**<br>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. |

**Tabelle 3: Erhöhter Schutzbedarf aus der SCHUBAN**

Damit ist für BVTax ein erhöhter Schutzbedarf ausgewiesen.

## 4.1 Risikomanagementmethode zur Reduktion nachrichtendienstlicher Ausspähung (RINA Prüfprozess)

Verschiedene Nachrichtendienste verfolgen eine umfassende Strategie der Informationsbeschaffung. Diese Nachrichtendienste können die IKT-Industrie in ihrem Land verpflichten, vertraglich festgehaltene und/oder gesetzlich vorgeschriebene Geheimhaltungspflichten nicht einzuhalten.
Die nachrichtendienstliche Ausspähung durch instrumentalisierte IKT-Firmen stellt aus sicherheitstechnischer Sicht nichts Neues dar: Die gängigen Angriffsmittel sind weiterhin vorsätzlich eingebaute Hintertüren (Backdoors) in der Hardware, in der Software oder in der Konfiguration, der missbräuchliche Zugriff auf Daten oder die Konfiguration eines IKT-Systems via Fernwartung und der direkte physische Zugriff. Insofern können alle IKT-Leistungen vom Consulting über die Planung und die Inbetriebnahme bis hin zu Support und Wartung davon betroffen sein.
Neu ist hingegen die Qualität der Angriffe, da die ausländischen Nachrichtendienste direkter, zielgerichteter und verdeckter die Vertraulichkeit, Integrität und Verfügbarkeit von Daten bedrohen können. Demzufolge bleiben die bisherigen sicherheitstechnischen und organisatorischen Schutzmassnahmen grundsätzlich wirkungsvoll, sie müssen jedoch ausgebaut werden. Aufgrund des Zugriffs durch ausländische Nachrichtendienste können externe/ausländische Leistungsersteller nicht mehr im gleichen Umfang wie früher als Sicherheitspartner angesehen werden.

### 4.1.1 Kriterien

Gestützt auf die in der Tabelle aufgeführten Kriterien, muss davon ausgegangen werden, dass der Geschäftsprozess inkl. der IKT-Objekte als risikorelevantes Schutzobjekt gilt.

| | |
|---|---|
| **Kriterium 1** | **Gegenseitige Abhängigkeiten mit anderen IKT-Infrastrukturen**<br>Das Schutzobjekt hat gegenseitige Abhängigkeiten mit anderen IKT-Infrastrukturen, wodurch diese **erheblich gefährdet** werden können. |
| **Kriterium 2** | **Das IKT-Schutzobjekt ist einer der fünf risikorelevanten Kategorien zuzuordnen**<br>1. Bereits die Ausschreibung ist sensitiv[3]: Bekanntgabe der geplanten Beschaffung ist bereits risikorelevant; Bekanntgabe der technischen Spezifikationen in der Ausschreibung ist bereits risikorelevant.<br>2. Outsourcing von Dienstleistungen, wo sensitive Daten faktisch und unumgänglich die Systeme der Bundesverwaltung verlassen (Betrieb/Support, Wartung):<br>• Managed Services (Risiko durch Verlust der Vertraulichkeit, Integrität und Nach-vollziehbarkeit): Daten werden externen IKT-Anbietern zur weiteren Verarbeitung/Operationalisierung übergeben;<br>• Managed Services (Risiko aufgrund der Beeinträchtigung der Verfügbarkeit durch nachrichtendienstliche Tätigkeit): Operationalisierungen/Prozesse/Dienstleistungen werden integral nach aussen gegeben.<br>3. Betriebsleistungen sowie Auf- und Abbauleistungen an internen kritischen Infrastrukturen mit autorisiertem Zugang zur zentralen Infrastruktur oder zu Applikationen: |

[3] Sensitiv heisst hier, dass die Schutzwürdigkeit von Informationen oder IKT-Prozessen bezüglich Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit erhöht ist.

| | |
|---|---|
| | • Remote Inbetriebnahme mit Zugang zu Daten bzw. zum zentralen Management-system der Infrastruktur bzw. Applikation;<br>• Remote Wartung oder Support mit Zugang zu Daten bzw. zum zentralen Managementsystem der Infrastruktur/Applikation, inklusive die Möglichkeit, Daten weg zu kopieren;<br>• On-Site Inbetriebnahme mit Zugang zu Daten bzw. zum zentralen Managementsystem der Infrastruktur/Applikation;<br>• On-Site Wartung oder Support mit Zugang zu Daten bzw. zum zentralen Managementsystem der Infrastruktur/Applikation.<br>• Bei diesem Kriterium sind auch die Aspekte betreffend möglicher Amtsgeheimnis-verletzung zu prüfen.<br>4. Beschaffung spezifischer besonders sensitiver IKT Infrastrukturen, vor allem für:<br>• Firewall, IPS (Intrusion Prevention System), IDS (Intrusion Detection System), Ap-plication Control, Anti-bot, Antivirus, Identity Awareness;<br>• Verschlüsselungsinfrastruktur inklusive Entwicklung, Support, Wartung, Audits mit Zugriff auf Kernapplikationen und vertrauliche Daten/Infos;<br>• IAM (Identity and Access Management)-Infrastruktur sofern korrumpierender Zu-griff auf Applikationen, Daten und Informationen möglich.<br>5. Risiko durch Zutrittsmöglichkeiten zu sensitiven Räumen, Gebäuden und IKT-Infrastrukturen ohne autorisierten Zugang zur zentralen Infrastruktur oder zu Applikationen. On-Site Wartung, Support, Inbetriebnahme mit physischem Zugang zu kritischen Räumlichkeiten (korrumpierende Zugriffsmöglichkeiten auf Räume, Gebäude und IT-Infrastruktur). |
| | |
| **Kriterium 4** | **Schutzbedarfsanalyse, erhöhter Schutzbedarf**<br>Weist die Schutzbedarfsanalyse einen erhöhten Schutzbedarf aus, ist eine Risikoanalyse durchzuführen. Die entsprechende Vorlage ist in den ISDS-Konzept-Unterlagen abgelegt. Im Falle einer RINA-Relevanz dient diese als Beurteilungshilfe der Kritikalität des Schutzobjektes und sollte in der Initialisierungsphase (gemäss HERMES) vorgenommen werden. |

BVTax hat zwar gegenseitige Abhängigkeiten zu kantonalen IKT Infrastrukturen, aber es sind keine direkten Zugriffe aus BVTax auf kantonale Systeme möglich. Aus diesem Grund ist eine erhebliche Gefährdung der kantonalen IKT-Infrastrukturen auszuschliessen.
Mit BVTax werden auch keine Personendaten verarbeitet.

**Gestützt auf die obigen Aussagen ist aus unserer Sicht eine RINA Relevanz nicht gegeben.**

# 5 Sicherheitsrelevante Systembeschreibung

Diese Kapitel beschreibt die sicherheitsrelevanten Elemente aus dem System, den Anwendungen, den vorhandenen und bearbeiteten Datensammlungen und den dazugehörenden Prozessen.

## 5.1 Ansprechpartner / Verantwortlichkeiten

| Wer | Name |
|---|---|
| **Anwendungsverantwortlicher** | Michael Baeriswyl, Delegierter SSK Ressort Informatik |
| **Inhaber der Daten** | Dr. Felix Sager, Ressort Logistik/Informatik SSK |
| **Systembetreiber LE** | Matthias Scheurer, BIT |
| **Anwendungsbetreiber LE** | Werner Zecchino, emineo AG |
| **Projektleiter LB** | Michael Baeriswyl, Delegierter SSK Ressort Informatik |
| **ISDS-V** | Dr. Felix Sager, Ressort Logistik/Informatik SSK |
| **ISBO** | Matthias Schwaller, ESTV |
| **DSBO** | Dr. Felix Sager, Ressort Logistik/Informatik SSK |
| **Benutzerkreis** | Fachstellen aus allen kantonalen Steuerverwaltungen |
| **weitere Stellen** | Keine |
| | |

## 5.2 Informationssicherheit

In der Informationssicherheit ist eine stetige Verbesserung der Sicherheitsmassnahmen sehr wichtig! Die Sicherheitsmassnahmen müssen laufend überprüft, verbessert und korrigiert werden.

Dazu bietet sich der PDCA-Zyklus[4] als Systematik zur kontinuierlichen Verbesserung bestens an.

[4] Demingkreis oder auch Deming-Rad, Shewhart Cycle nach William Edwards Deming


Nur wenn dieser Zyklus auch tatsächlich gelebt wird, können wir die Informationssicherheit laufend verbessern.

## 5.3 Beschreibung des Gesamtsystems

Das System BVTax (Business Valuation Tax) ermöglicht den Kantonen (Steuerverwaltungen) 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.

Die folgenden Erweiterungen wurden realisiert:
- Auskunftsfunktion für die Abfrage von NKT Steuerwerten
- Stellen und Verwalten von Bewertungsaufträgen

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 Bundes. 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 (für Daten der ESTV von ICTax und Core-IT).
- 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 Grundstückdaten sowie für die Archivierung der Eröffnungsschreiben.

BVTax wird durch das BIT in der Cloud Foundry (Atlantica) betrieben. In BVTax werden verschieden OpenSource und proprietäre Technologien eingesetzt. Die Details sind aus dem Dokument "BVTAX Systemarchitektur-v21-20200520_112736" ersichtlich.

## 5.4 Beschreibung der zu bearbeitenden Daten

In der Anwendung BVTax werden die folgenden Daten bearbeitet:

- Stammdaten zu nicht kotierten Gesellschaften
- Stammdaten zu nicht kotierten Titeln
- Stammdaten zu nicht kotierten ausländischen Gesellschaften
- Stammdaten zu nicht kotierten ausländischen Titeln
- Ereignisse und Erträge zu nicht kotierten Titeln
- Bewertungen von nicht kotierten Gesellschaften
- Steuerwerte zu nicht kotierten Gesellschaften
- Benutzer, Rollen und Berechtigungen

Für BVTax besteht die gesetzliche Grundlage in der Form der Bundesgesetze über die direkte Bundessteuer und die Verrechnungssteuer (vgl. Kap. 3).

Aufgrund der Anbietepflicht der Bundesämter gegenüber dem Bundesarchiv (BAR) müssen die Daten zu gegebener Zeit dem BAR zur Archivierung angeboten werden. Das BAR entscheidet dann, ob die Daten als archivwürdig bewertet und zur Archivierung übernommen werden.

Da mit BVTax Personendaten bearbeitet werden, muss die Datensammlung beim EDÖB angemeldet werden.

Da verschiedene kantonale Behörden mit BVTax arbeiten und Schnittstellen zu kantonalen und ESTV-Systemen bestehen wird empfohlen ein «abgespecktes» Datenbearbeitungsreglement zu erstellen.

## 5.5 Architekturskizze / Systemübersicht

Die nachfolgende Systemübersicht zeigt BVTAx mit den Schnittstellen und den Umsystemen.

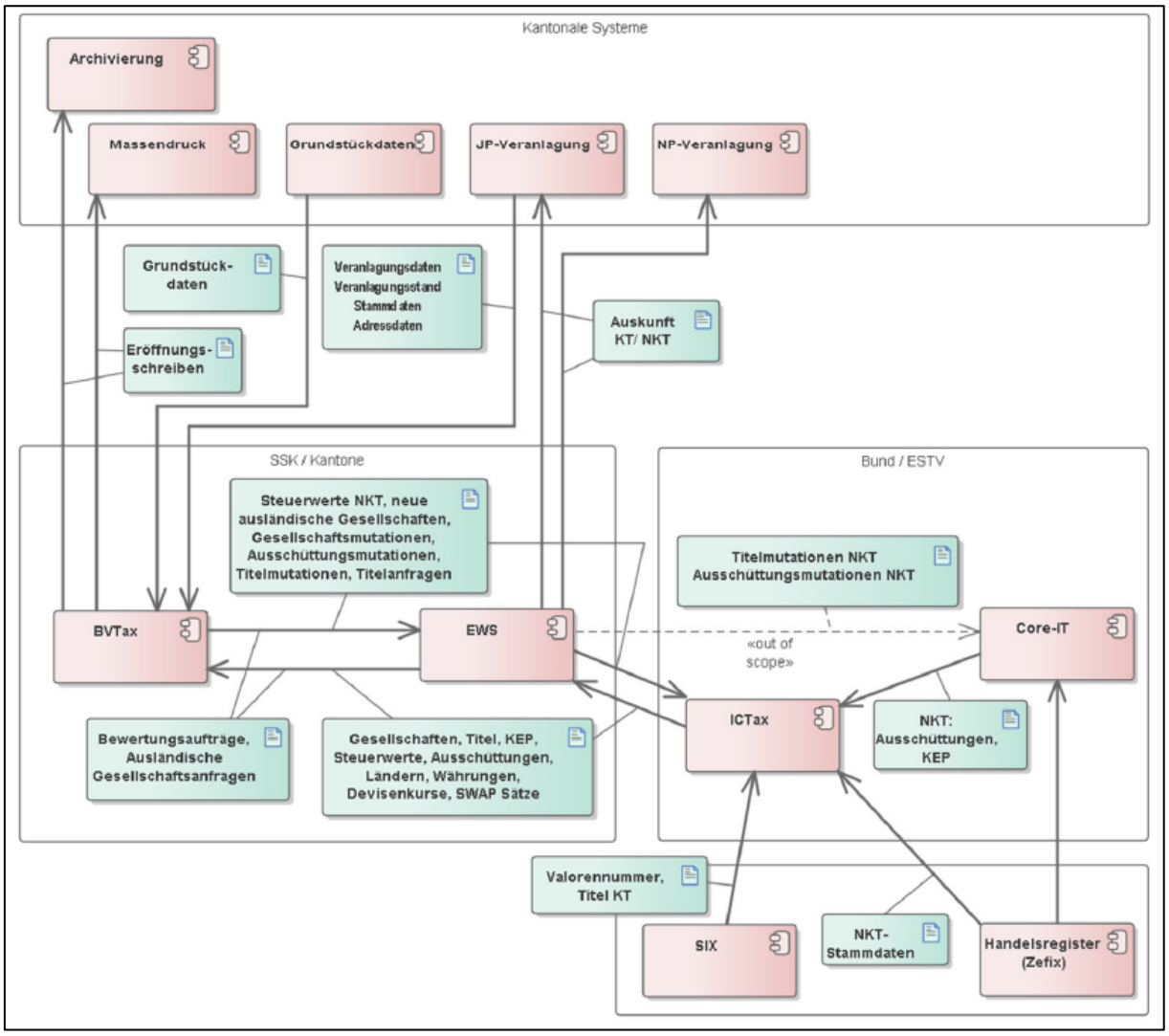



**Abbildung 1: Systemübersicht BVTax mit Schnittstellen zu Umsystemen**

Die BVTax-Architekturskizze des BIT findet sich im Anhang 11.

## 5.6 Beschreibung der zugrundeliegenden Technik

Die eingesetzten Technologien bauen auf den Vorgaben des ISB bzw. des NCSC auf und umfassen Open-Source und proprietäre Technologien. Die Systemarchitektur ist im Dokument "BVTAX Systemarchitektur-v21-20200520_112736" mit den eingesetzten Technologien und Versionen im Detail beschrieben (vgl. Kap.4).

Die Anwendung BVTax wird durch das BIT in der Cloud Foundry gehostet. Die Verantwortung für die BVTax Anwendung liegt bei der emineo AG.

Die Anwendung BVTax interagiert mit den Benutzern über ein Web-Frontend sowie mit externen Systemen über WebService-Schnittstellen. Die Applikation ist als Standard 3-Schichten (3-tier) Applikation realisiert, wobei die Präsentations-Schicht (Frontend) im Web-Browser läuft und mit Typescript/Angular umgesetzt wird. Die Geschäftslogik im Backend wird mit Java/Spring umgesetzt.

Die Kommunikation zwischen Client-Server wird in der gesamten Anwendung über TLS 1.2 verschlüsselt. Die Authentisierung der auf BVTax erfolgt über eIAM des Bundes. eIAM vergibt eine Auto-Grant-Rolle, die Rollen, die Berechtigungen innerhalb des Systems steuern, werden in BVTax direkt verwaltet. Die Autorisierung (Rollen-basiert) ist mit Hilfe von Spring Security umgesetzt und wird von berechtigten Systemadministratoren verwaltet.

Die Nachvollziehbarkeit wird sowohl technisch (z.B. Protokollierung der Logins) als auch fachlich (z.B. Protokollierung aller Datenmutationen) sichergestellt. Die Logdateien werden in der Anwendung BVTax gespeichert. Die Aufbewahrungsfrist ist gemäss der «Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen» geregelt und auf 2 Jahre beschränkt.

Für alle Schnittstellen zu BVTax wird das SOAP-Protokoll über TLS-verschlüsselte HTTPS-Verbindungen verwendet.

Grundlage der Lösung ist die BIT "Atlantica" Cloud Foundry PaaS (Container) und die IaaS (VM) Plattform. Die Container und VMs befinden sich in der SSZ-Netzwerkzone (SK1). Dadurch ist ein direkter Zugriff auf kantonale Systeme nicht möglich.

**Integration kantonaler Systeme**

BVTax benötigt für verschiedene Themen Schnittstellen zu kantonalen Systemen.

Die folgenden Daten werden für die Bewertung verwendet und sind auf kantonalen Systemen verfügbar:

- JP-Veranlagungsdaten
- Grundstückdaten

Für die folgenden Funktionen müssen Daten aus BVTax an die Kantone geliefert werden:

- Massendruck Eröffnungsschreiben
- Archivierung

BVTax wird als Web-Applikation im Bundesnetz (Shared Service Zone des BIT) betrieben und nicht wie die Vorgängerapplikation WVK als Client-Installation in den kantonalen Netzen. Dadurch ist ein direkter Zugriff auf kantonale Systeme nicht möglich.

Der Aufruf der Schnittstellen erfolgt immer aus einem kantonalen System.
Für Schnittstellen, bei denen kantonale Systeme Daten an BVTax liefern, erstellt BVTax jeweils einen Request für einen Datensatz, wenn dieser durch einen Bewerter benötigt wird. Dieser wird von einem kantonalen System abgeholt und die entsprechenden Daten soweit verfügbar geliefert. Daten können von den kantonalen Systemen auch ohne Request seitens BVTax geliefert werden.

Bei Daten, die durch die Kantone von BVTax bezogen werden (Eröffnungsschreiben, Archivierung und Massendruck) sind die Kantone unabhängig in der Auslösung der Abholung.

Das folgende Diagramm illustriert die Datenflüsse bei einer providerseitigen Schnittstelle auf BVTax. Auf kantonaler Seite bestehen dabei verschiedene Möglichkeiten, die Schnittstelle anzubinden:

- direkte einzelne Anbindungen (Kanton A)
- Anbindung über eine zentrale Datensammelstelle (Kanton B)
- Teilanbindung von einzelnen Datenquellen (Kanton C)

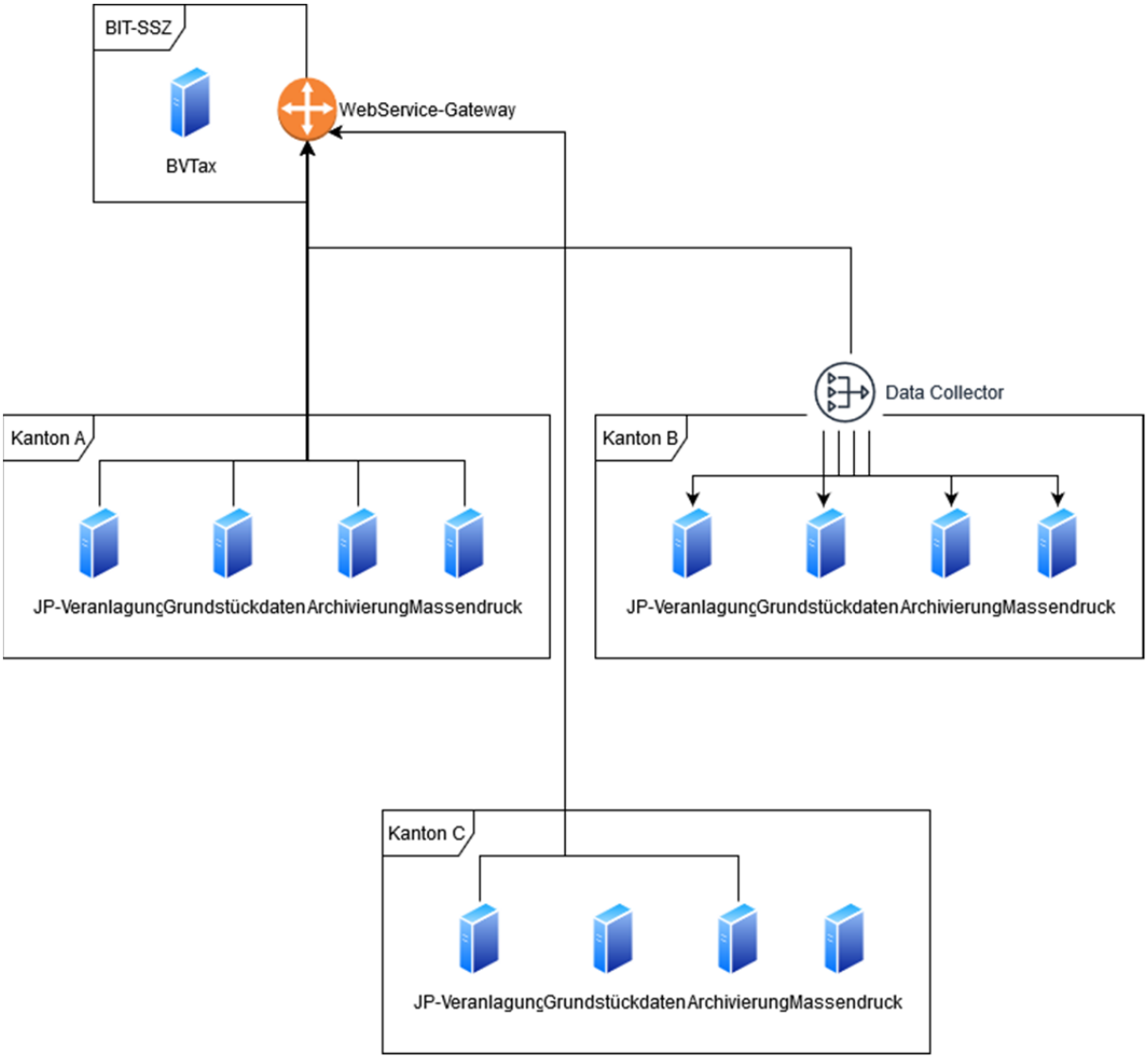



**Abbildung 2: Datenflüsse bei einer serverseitigen Schnittstelle auf BVTax**

## 5.7 Rollen und Berechtigungen

Der Zugriff auf BVTax erfolgt ausschliesslich über das Identity und Access Management (eIAM) des BIT gemäss den Vorgaben. Die Zugriffsberechtigungen werden basierend auf dem Rollenkonzept vergeben. Mittels den Objekten Benutzer, Gruppe und Rolle wird festgelegt, welche Funktionalitäten ein Benutzer in der BVTax Anwendung ausführen darf und auf welche Daten er Zugriff hat. BVTax wird hinter dem eIAM des Bundes betrieben. eIAM übernimmt dabei die Funktionalität der Authentisierung für die Verwendung von BVTax. eIAM stellt sicher, dass nur die in eIAM mit der im ISDS Konzept definierten Authentisierungsstärke authentisierten Benutzer auf BVTax zugreifen können. Deshalb muss jeder BVTax Benutzer in eIAM vorhanden sein. Mittels einer generellen BVTax eIAM Autorolle erhält der Benutzer Zugriff auf die BVTax Anwendung. Der Benutzer dient auch dazu, die Person, welche eine Aktion in BVTax ausführt zu identifizieren.

Benutzer werden nach einer Inaktivität von 60 Tagen im System automatisch gelöscht. Dies bedingt aber, dass die für die Benutzerverwaltung zuständigen Stellen die Mutationen zeitnah nachführen.

eIAM verwendet vier Authentisierungsstufen:

| Authentisierungslevel | Authentisierungsmittel |
|---|---|
| **auth.guest** | • SMS-Code |
| **auth.weak** | • Passwort (verschlüsselt übertragen) |
| **auth.normal** | • Passwort (verschlüsselt übertragen) & SMS-Code<br>• Passwort (verschlüsselt übertragen) & OTP (Vasco)<br>• Kerberos<br>• Swiss Government PKI (SG-PKI) Class D Zertifikat (Soft Zertifikat) |
| **auth.strong** | • Passwort (verschlüsselt übertragen) & OTP (Vasco)<br>• SuisseID<br>• Swiss Government PKI (SG-PKI) Class B Zertifikat (Smart Card oder USB Stick) |

**Abbildung 3: eIAM Authenthisierungsstufen[5]**

Für BVTax gilt die Stufe **auth.strong**, d.h. für die Authentisierung der Benutzer wird entweder ein Token oder ein Zertifikat benötigt.

Während eIAM den Benutzer generell für die BVTax Anwendung autorisiert, erfolgt die Autorisierung für einzelne Funktionen innerhalb der Anwendung direkt durch BVTax anhand der Berechtigungen.

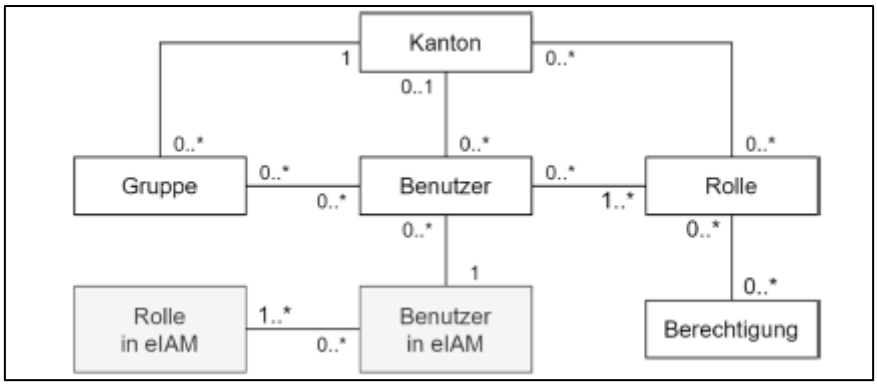



**Abbildung 4: BVTax eIAM-Rollen**

[5] gem. https://www.eiam.admin.ch/r/P/_7892316076_Integration_Applikationen_eIAM_SAML2.0.pdf?t=1579180103

Nachfolgend sind die für BVTax relevanten Businessrollen als Übersicht aufgeführt und beschrieben. Mit Ausnahme des VIP-Bewerters werden alle Businessrollen auch als Applikationsrollen hinterlegt. Die VIP-Bewerter-Businessrolle wird speziell behandelt, da sie nicht einer allgemeinen Applikationsrolle entspricht, sondern gesellschaftsspezifisch vergeben wird.

| Rolle | Beschreibung |
|---|---|
| Administrator Ausländische Gesellschaft | Bei der Rolle «Administrator Ausländische Gesellschaft» handelt es sich um ein interkantonales Team, welches verantwortlich ist für die Erfassung und Mutation von ausländischen Gesellschaften. |
| Administrator Kanton | Spezifische Funktionen innerhalb von BVTax stehen dem kantonalen Administrator zur Verfügung |
| Administrator SSK | Der Administrator der SSK verwaltet spezifische Konfigurationen innerhalb von BVTax. Der Administrator der SSK hat keinen Zugriff auf bewertungsrelevante Informationen. |
| Auftraggeber | Beim Auftraggeber handelt es sich um einen Mitarbeiter der kantonalen Steuerbehörde, der einen Auftrag für die Bewertung eines nicht kotiertenTitels oder eine ausländische Gesellschaftsanfrage stellt. |
| Bewerter | Der Bewerter ist ein Mitarbeitender der kantonalen Steuerbehörde, welcher die nicht kotierten Gesellschaften auf Grundlage des Kreisscheiben Nr. 28 bewertet. |
| Bewerter AVOR | Der Bewerter AVOR (Arbeitsvorbereitung) ist ein Mitarbeitender der Kantonalen Steuerbehörde, welcher die vorbereitenden Arbeiten für die Bewerter durchführt. Beispielsweise die Zu- und Umteilung von Bewertungsaufträgen, Auskunftserteilung etc. |
| Bewerter Lead | Der «Bewerter Lead» ist ein Mitarbeitender der kantonalen Steuerbehörde, welcher die nicht kotierten Gesellschaften auf Grundlage des Kreisscheiben Nr. 28 bewertet. Zusätzlich ist er verantwortlich für die ihm zugeordnete Struktur (regionale Struktur, organisatorische Struktur) etc. |
| Bewerter VIP | Der Bewerter ist ein Mitarbeitender der kantonalen Steuerbehörde, welcher die nicht kotierten Gesellschaften auf Grundlage des Kreisscheiben Nr. 28 bewertet. |

**Tabelle 4: Rollen und Berechtigungen**

Die Details sind aus dem Dokument «BVTAX Rollen- und Berechtigungskonzept-v24-20200815_141116» ersichtlich.

# 6 Risikoanalyse und Schutzmassnahmen

## 6.1 Restrisiken

Nachfolgen die Übersicht über die Restrisiken, die Details dazu finden sich im Dokument RISIKOANALYSE.

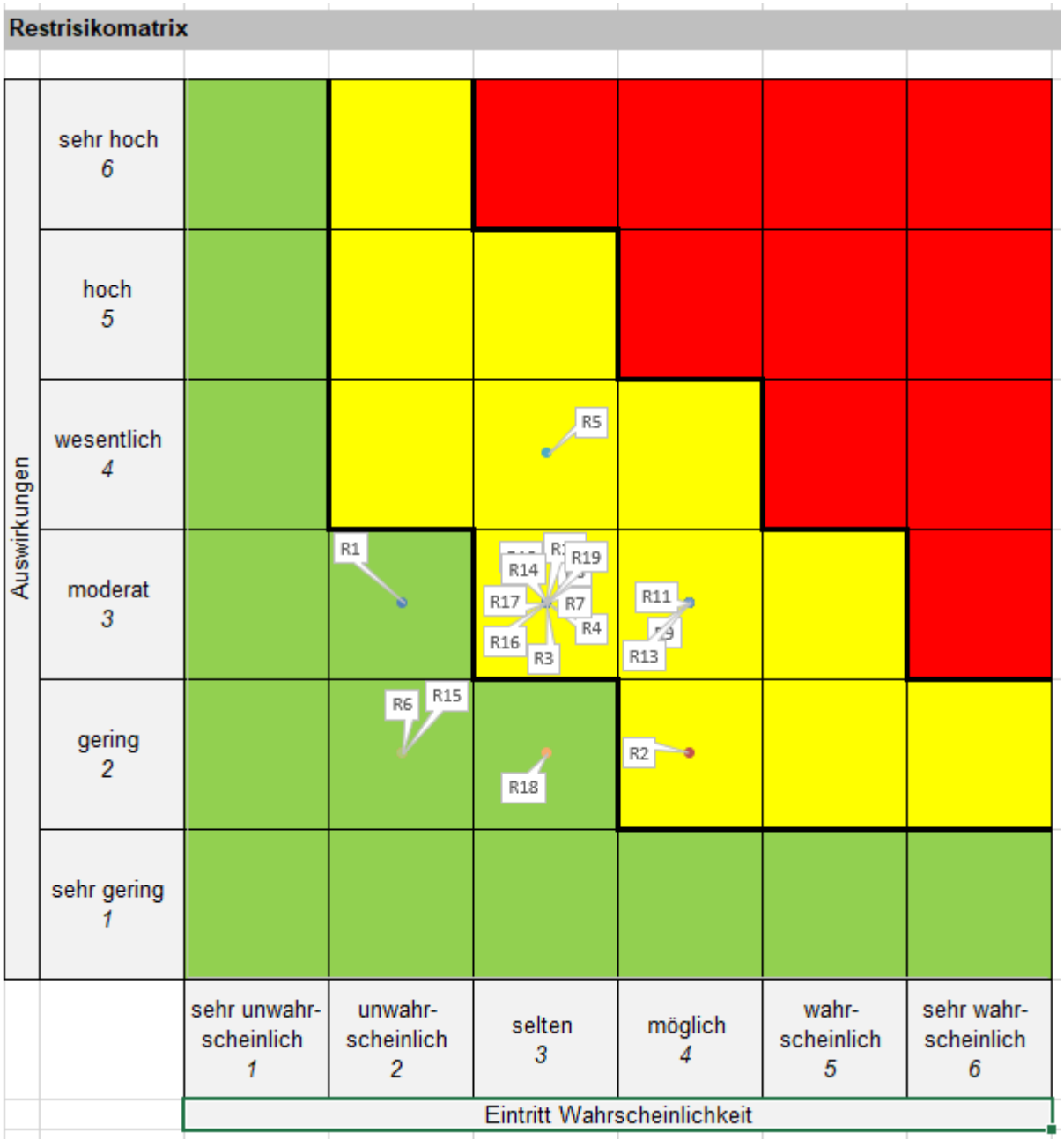



**Abbildung 5: Restrisikomatrix aus BVTax-ISDS-Sicherheitsanalyse**

Die Restrisiken umfassen zwei Gruppen:

1. Die Risiken aus der Überprüfung der IKT-Grundschutz Umsetzung [GRUNDSCHUTZ
2. Die Risiken aus der Risikoanalyse [RISIKOANALYSE]. Das dürfen nur gelbe Risiken sein. Bei roten Risiken müssen Massnahmen ergriffen werden.

Aus der Überprüfung der **IKT-Grundschutz Umsetzung** sind die folgenden Restrisiken übrig geblieben:

| Nr. | Sicherheitsanforderung | Vorgeschlagene Massnahme |
|---|---|---|
| 2.1.1 | Nur Smart Devices, welche über ein Mobile Device Management (MDM) verwaltet werden, dürfen mit Systemen der Bundesverwaltung kommunizieren. | Der Einsatz von mobilen Geräten ist für BVTax nicht vorgesehen. Sollte der Einsatz von (privaten) Tablets zugelassen werden, dann erfolgt der Zugang über eIAM mit 2 Faktor Authentisierung via SMS-Code. |
| 7.1.7 | Der Zugriff von Personen auf Arbeitsplatz- und Serversysteme der Bundesverwaltung darf nur über eine 2-Faktor-Authentisierung möglich sein. | Mit der eIAM-Integration wird sichergestellt, dass die Authentifizierung den Vorgaben entspricht. |
| 9.2 | Die Administration von Serversystemen erfolgt auf einem (logischen) getrennten Administrationsnetz und ist über dedizierte und gesondert abgesicherte IKT-Systeme auszuführen. Dieses Netz darf keinen Zugriff zum Internet und zur Bürokommunikation (i.e. Mailbox) haben. Wenn technisch nicht umsetzbar, muss die Art und Weise des Administrationszugangs in einem ISDS-Konzept beschrieben werden.<br>Für den Zugriff auf diese administrative Managementebene bzw. auf die zu administrierenden Zielsysteme ist eine 2-Faktor-Authentifizierung umzusetzen. | Die BVTax Serversysteme sind nur durch berechtigte Administratoren aus dem BIT erreichbar. Mit der eIAM-Integration wird sichergestellt, dass die Authentifizierung den Vorgaben entspricht. |
| 8.2<br>8.3<br>8.4<br>12.1.3<br>16.1 | Ein Organisationshandbuch muss vor Inbetriebnahme fertiggestellt und freigegeben werden. | Das Organisationshandbuch (OHB) muss für BVTax unter Mitwirkung von LE (BIT und emineo AG) und LB erstellt und vom Auftraggeber freigegeben werden. |
| 7.1.9<br>13.1.7 | Datenzugriffe auf BVTax dürfen nur verschlüsselt erfolgen. Die Daten sind bei der Übertragung zu verschlüsseln.,. | Alle Zugriffe erfolgen verschlüsselt mit HTTPS und SSL/TLS (TLS 1.2)<br>*Hinweis:* Aufgrund einer Sicherheitslücke dürfte das BIT auf TLS 1.3 umstellen |
| 14.2.1 | Testdaten sind entsprechend ihrer Einstufung zu schützen.<br>Ist es unumgänglich, dass produktive Daten zu Testzwecken verwendet werden, sind diese gemäss ihrer Einstufung zu schützen. | Ist durch die LE (BIT und emineo) technisch und organisatorisch sichergestellt.<br>Der Standort der Entwicklungs- und Testumgebung (Server und Datenbanken) in der Schweiz ist sicherzustellen. |

**Tabelle 5: Restrisiken aus der Überprüfung der IKT-Grundschutz Umsetzung**

Aus der **Risikoanalyse** bestehen keine grossen Risiken (Rot) deren Auswirkungen kritisch bis katastrophal sind.

Von den Risiken deren Auswirkungen erheblich sind (Gelb) und die deshalb zu reduzieren sind, werden die Punkte unten beschrieben.

Die nachfolgenden Risiken im gelben Bereich sind:

| Nr. | Risiko | Begründung/Massnahme |
|---|---|---|
| R2 | Ausfalls von Stromversorgung oder Kommunikationsnetzen | komplexes System, Abhängigkeiten<br>*Massnahme:*<br>Die Systeme sind laufend zu überwachen (Monitoring) |
| R3 | Ausfall oder Störung von Dienstleistern | Schlüsselpersonen nicht verfügbar<br>*Massnahme:*<br>Stellvertretung und Knowhow Sicherung und Zugang ist sicherzustellen |
| R4 | Ausspähen von Informationen, Spionage, Abhören | Ungenügend vor unerlaubtem Zugriff geschützt<br>*Massnahme:*<br>Der Zugang ist nur auf berechtigte Benutzer beschränkt und erfolgt über eIAM mit 2-FA |
| R5 | Diebstahl oder Verlust von Geräten, Datenträgern oder Dokumenten | Datenverlust durch hohes Datenvolumen<br>*Massnahme:*<br>Daten sind zu verschlüsseln und bei Ereignissen gilt der definierte Incident-Prozess |
| R7 | Manipulation von Informationen, Hard- oder Software | Fahrlässigkeit, unbeabsichtigte Beschädigung durch Administratoren<br>*Massnahme:*<br>Risikominderung durch definierte Prozessablaufe und kontrollierte Einhaltung. |
| R8 | Zerstörung, Ausfall oder Fehlfunktion von Geräten oder Systemen | Fahrlässigkeit, unbeabsichtigte Beschädigung durch Administratoren<br>*Massnahme:*<br>Mit entsprechenden Massnahmen (Monitoring, etc.) kann das Risiko vermindert werden. |
| R9 | Softwareschwachstelle oder -Fehler | nicht Patchen des Systems, Fehlerhafte Releases, fehlerhafte Patches (ungenügendes Testing)<br>*Massnahme:*<br>Mit Wartungsverträgen sind die Reaktions- und Fehlerbehebungszeiten definiert |
| R10 | Verstoss gegen Vorschriften oder Regelungen | Nicht Einhaltung der Vorgaben und Prozesse, mangelnde Schulung<br>*Massnahme:*<br>Mit organisatorischen Massnahmen kann dieses Risiko minimiert werden. Risikominderung durch definierte Prozessablaufe und Tracking. |
| R11 | Unberechtigte oder fehlerhafte Nutzung oder Administration von Geräten und Systemen, Missbrauch von Berechtigungen | Verletzung der Integrität und Datenschutz<br>*Massnahme:*<br>Der Zugang ist nur auf berechtigte Benutzer beschränkt und erfolgt über eIAM mit 2-FA. Die Systeme sind laufend zu überwachen (Monitoring) |
| R12 | Personalausfall | Schlüsselpersonen nicht verfügbar |

| | | |
|---|---|---|
| | | *Massnahme:*<br>Durch Wartungsverträge mit den LE (BIT und emineo AG) sind im SLA auch die Massnahmen bei Personalausfall z.B. Stellvertretungen, Ersatz, etc. geregelt. |
| R13 | Missbrauch personenbezogener Daten | Unberechtigter Zugriff, Betrugsversuche<br>*Massnahme:*<br>Risikominderung durch eIAM mit 2FA und durch aktives Monitoring. |
| R14 | Verhinderung von Diensten (Denial of Service), Sabotage | Insider Angriff<br>*Massnahme:*<br>Die Systeme sind laufend zu überwachen (Monitoring) |
| R16 | Datenverlust | Ungenügend getestetes Backup/Restore<br>*Massnahme:*<br>Die Backup-/Restoreprozesse sind periodisch zu testen |
| R17 | Informationsabfluss über Umsysteme | Backup ist nicht Verschlüsselt, unkontrollierte Datenexporte durch Entwicklung und Support<br>*Massnahme:*<br>Mit organisatorischen Massnahmen kann dieses Risiko minimiert werden. Die Systeme sind laufend zu überwachen (Monitoring) |
| R19 | Ausfall der Umsysteme / Basisinfrastruktur | Ausfall der Basissysteme<br>*Massnahme:*<br>Die Systeme sind laufend zu überwachen (Monitoring) |

**Tabelle 6: Restrisiken aus der Risikoanalyse**

Die Restrisiken sind mit den vorgeschlagenen Massnahmen zu reduzieren. Auch die fortlaufende Umsetzung der Schutzmassnahmen ist zu kontrollieren.

## 6.2 Fortlaufende Umsetzung der Schutzmassnahmen

Pro Massnahme dokumentiert ist die für die Umsetzung verantwortliche Person und wo sinnvoll die Art der Umsetzung (z.B. Häufigkeit von Prüfungen) und wie die Umsetzung nachgewiesen wird (zu führende Protokolle etc.). Die Liste umfasst nur diejenigen Massnahmen, deren Umsetzung durch den BVTax Anwendungsverantwortlichen beauftragt und überprüft wird. Ergänzungen in der Liste haben zur Folge, dass auch im Originaldokument «Risikoanalyse» Anpassungen nötig werden und eine neu-Beurteilung der Risiken zur Folge haben.

Die Umsetzung der Schutzmassnahmen wird teilweise redundant sowohl im ISDS-Konzept als auch im Bearbeitungsreglement (Datenschutz) dokumentiert.

Das Nachführen dieser Massnahmenliste ist die Aufgabe des Anwendungsverantwortlichen oder/und der Geschäftsprozessverantwortlichen. Die Massnahmen sind regelmässig mit dem ISBO abzustimmen.

| Nr. | Massnahmen | Verant-wortlich | Umsetzung / Dokumentation / Bestä-tigung |
|---|---|---|---|
| 1 | Einhaltung des IKT Grundschutz IKT Grundschutz ist wie Dokumentiert umgesetzt | ISBO | Laufende Umsetzung |
| 2 | OWASP Top Ten Risiken wurden bei der Entwicklung berücksichtig | PL-LB | |
| 3 | Sensibilisierung und Schulung der MA im Bereich Informationssicherheit | Anwendungsverantwortlicher | |
| 4 | Unzureichende Kenntnis über Regelungen | LB/LE | Organisationshandbuch und Schulung |
| 5 | Ausreichende Ressourcen für den IT-Betrieb BVTax | LE | |
| 6 | Zeitnahes Patch- und Änderungsmanagement, genügende Ressourcen für Patchen | LE | |
| 7 | Schutz vor SQL-Injection | LE | |
| 8 | Sichere Konfiguration von Webanwendungen | LE | |
| 9 | Sichere HTTP-Konfiguration bei Webanwendungen | LE | |
| 10 | Überprüfung von Webanwendungen / Regelmässiger Security PEN Tests | LE | |
| 11 | Kryptografische Sicherung vertraulicher Daten | LE | |
| 12 | Verwenden von qualitativ guten Passwörtern. Einhaltung der Passwortregeln | LE | |

**Tabelle 7: Massnahmenliste**

Weitere Massnahmen können jederzeit definiert werden. Sie sind mit dem ISBO abzustimmen.

## 6.3 Potenzielle sicherheitsrelevante Vorfälle

Die Anwendung BVTAX führt ein Log wichtiger Ereignisse. Dieses Log kann z.B. vom Sicherheitsbeauftragten ISBO oder DSBO analysiert werden, um potentiell sicherheitsrelevante Vorfälle zu identifizieren. Das BIT bietet eine Dienstleistung «Analyse/Monitoring» des Netzwerkverkehrs an. Bei Bedarf ist abzuklären, ob diese Dienstleistung auch für die Log-Analyse genutzt werden kann.

Aus Sicht ISBO können folgende Vorfälle eine Analyse erfordern (Liste nicht abschliessend):

| Vorfall | Kriterien |
|---|---|
| Unverhältnismässige Erweiterung der Zugriffsrechte | Derselbe Benutzer ist oder wird überdurchschnittlich vielen Rollen zugeordnet. |
| Massiver Download / Export | Derselbe Benutzer greift in einem kurzen Zeitraum auf viele Dokumente verschiedener Geschäfte zu |

| Vorfall | Kriterien |
|---|---|
| Manipulieren der Daten bei der Eingabe | Benutzer können uneingeschränkt die Daten in der Applikation verändern |
| Daten nicht mehr verfügbar | Die Daten sind nicht mehr verfügbar oder zerstört und können aus dem Backup nicht wiederhergestellt werden. |
| Schlüsselpersonen sind nicht verfügbar | Wissensträger stehen nicht zur Verfügung. Dies kann zu Verzögerungen führen. Ein Zugriff auf die Persönlichen Ordner und das Postfach kann unumgänglich werden. |
| Unberechtigte Person in den Räumlichkeiten | Durch mangelnde Gebäudesicherheit oder menschliches Fehlhandeln können sich unberechtigte/fremde Personen in den Räumlichkeiten aufhalten und so die Informationssicherheit gefährden. |
| | |

**Tabelle 8: Liste der möglichen Sicherheitsrelevanter Vorfälle**

# 7 Wiederherstellung des Geschäftsbetriebes

Gemäss Einschätzung des PL-LB ist für BVTax ist kein Notfallkonzept zu erstellen da es sich nicht um eine Anwendung mit kritischen Geschäftsprozessen handelt.

Die zeitliche Ausfalldauer nach einem Vorfall der einen Datenrestore zur Wiederherstellung des Geschäftsbetriebes notwendig macht, ist mit dem LE BIT im Rahmen des SLAs vertraglich abzudecken.

# 8 Einhaltung / Überprüfung / Abnahme der Schutzmassnahmen

## 8.1 Allgemeines

Die Einhaltung, Überprüfung und Abnahme der Schutzmassnahmen im Rahmen einer Sicherheitsüberprüfung ist regelmässig alle 5 Jahre zu wiederholen oder bei wesentlichen Anpassungen im EWV-Systemverbund oder in der Applikation BVTax.

Eine ausserordentliche Überprüfung ist nach der Umsetzung der eIAM-Integration bzw. Anpassung der Verfügbarkeitsstufe durchzuführen.

Das ISDS-Konzept muss periodisch überprüft werden und zwar vom ISBO der ESTV zusammen mit den Verantwortlichen des LE (BIT) und des LB (SSK-Vertreter). Zuständigkeiten gemäss den definierten Betriebsprozessen. Abnahme durch Betrieb ist erfolgt.

Vom LE wird verlangt, bevor die Applikation produktiv geschaltet wird, dass dieser mit geeigneten Werkzeugen und Tools die Applikation und die Datenbanken auf Sicherheitslücken und Manipulierbarkeit testet und ein entsprechendes Protokoll führt. Das Protokoll und die Resultate sind innert nützlicher Frist (nach Abschluss der Tests) dem ISBO der ESTV und BIT unaufgefordert zukommen zu lassen. Diese Tests und entsprechende allfällige Korrekturmassnahmen sind vor dem Einführungsdatum/Produktivschaltung vollumfänglich abzuschliessen.

Die Teste sind mit dem LE (BIT) im Rahmen von DLVs zu planen und zu vereinbaren.

Verantwortlich für die Umsetzung der Sicherheitsmassnahmen sind der Anwendungsverant-

wortliche und der Inhaber der Datensammlungen in Abstimmung mit dem ISBO.

## 8.2 Aufrechterhaltung der Sicherheitsmassnahmen im laufenden Betrieb

Die Sicherheitsmassnahmen müssen laufend auf ihre Wirksamkeit, Aktualität und der täglichen Praxis überprüft- und angepasst werden.
Veränderungen der Bedrohungslage oder durch falsche Verwendung der implementierten Sicherheitsmassnahmen müssen erkannt und entsprechend Gegenmassnahmen eingeleitet werden.

Das Sicherheitsniveau lässt sich nur dann aufrechterhalten, wenn:

- Wartung und administrativer Support der Sicherheitseinrichtungen gewährleistet sind
- Die realisierten Massnahmen regelmässig auf ihre Übereinstimmung mit den Sicherheitsanforderungen geprüft werden
- Die IT-Systeme fortlaufend überwacht werden (Monitoring).

Von besonderer Wichtigkeit für die Aufrechterhaltung oder weitere Erhöhung eines einmal erreichten Sicherheitsniveaus ist eine permanente Sensibilisierung aller betroffenen Mitarbeiter/ innen für Fragen der Informationssicherheit.
Verantwortlich für diese Aktivitäten sind der Anwendungsverantwortliche und der Inhaber der Datensammlungen in Abstimmung mit dem Auftraggeber und dem ISBO.

Die Schutzmassnahmen sind wie folgt zu sichern:

1. Die neuen Funktionen werden durch ein Anforderungsassessment gegenüber der bestehenden Architektur sowie der SCHUBAN, dem IKT Grundschutz und ISDS Konzept verifiziert.
2. Die neuen Funktionen werden durch den LB spezifiziert und auch abgenommen.
3. Der Service Release durchläuft über das Staging Verfahren der Umgebungsarchitektur verschiedene Testsequenzen mit Qualitätschecks.
4. Durchführen eines regelmässigen Sicherheitschecks.
5. Wissenstransfer an die Betriebsorganisation.
6. Abnahmetestprotokoll und Go Life durch Anwendungsverantwortlicher des LB.
7. Produktivsetzung via das definierte Changemanagement Verfahren.

## 8.3 Systemabnahmeprüfung

Die Schutzmassnahmen müssen laufend auf ihre Wirksamkeit, Aktualität in der täglichen Praxis überprüft- und angepasst werden. Veränderungen der Bedrohungslage oder eine falsche Verwendung der implementierten Sicherheitsmassnahmen müssen erkannt werden und entsprechend Gegenmassnahmen eingeleitet werden.

Das Sicherheitsniveau lässt sich nur dann aufrechterhalten, wenn

- Wartung und administrativer Support der Sicherheitseinrichtungen gewährleistet sind
- Die realisierten Massnahmen regelmässig auf ihre Übereinstimmung mit den Sicherheitsanforderungen geprüft werden
- Die IT-Systeme fortlaufend überwacht werden (Monitoring)

Von besonderer Wichtigkeit für die Aufrechterhaltung oder weitere Erhöhung eines einmal erreichten Sicherheitsniveaus ist eine permanente Sensibilisierung aller betroffenen Mitarbeiter/ innen für Fragen der Informationssicherheit.

Verantwortlich für diese Aktivitäten sind der Anwendungsverantwortliche und der Inhaber der Datensammlungen in Abstimmung mit dem ISBO ESTV.

## 8.4 Zugriff auf bewirtschaftete Daten

Auf die bewirtschafteten Daten über die Mitarbeiter der ESTV (intern und extern) kann gestützt auf Art. 2 Abs.1 Bst. b der Randdatenverordnung (SR 172.010.442) nur der Informationssicherheitsbeauftragter der ESTV (ISBO oder DSBO) zugreifen. Falls andere Organisationseinheiten der ESTV Zugriff auf diese Daten benötigen, brauchen sie zwingend das Einverständnis der Amtsleitung. Vorgängig ist der Informationssicherheitsbeauftragte anzuhören.

## 8.5 Spezifische Kontrollen

Nachfolgend führt der ISBO getätigte Prüfungen und spezifischen Kontrollen im Bereich der Datensicherheit, Vertraulichkeit und Datenschutz durch.

| Nr. | Art der Kontrolle / Prüfung | Verant-wortlich | Feststellung / Dokumentation |
|---|---|---|---|
| 01 | Bestätigung Backup / Restore BVTax | LE | Die Zeitspanne eines umfangreichen Disaster Recovery variiert von<br>- 3-5 Stunden (falls nur BVTax betroffen ist) bis<br>- mind. 5 Arbeitstage, falls der ganze Galera Cluster gecrashed ist und alle 3 VMs neu aufgesetzt werden müssen (diese Zeitspanne berücksichtigt die Prozessdurchlaufzeiten des BIT und beruht auf den Erfahrungswerten). |

**Tabelle 9: Liste der Prüfungen und Kontrollen**

Mit einer Zusammenfassung des durchgeführten Audits (wer, wann, was, Resultat) wird die Umsetzung dokumentiert.

# 9 Ausserbetriebnahme

Die Liquidation ist nicht vorgesehen. Anstelle dessen wird Technologiemanagement durchgeführt.

Für die Applikation BVTax werden die Releasezyklen zu Programmiersprache, Datenbank, Betriebssystem und Sicherheitsupdates eingehalten. Um den Technologiewandel zu berücksichtigen, wird die Architektur regelmässig modernisiert oder bei passender Gelegenheit (~ alle 5 Jahre) ausgetauscht.

Der ISBO ESTV beschreibt die zu beachtenden Punkte bei einer Ausserbetriebnahme des/eines Systems wie folgt:

1. Alle geschäftsrelevanten Informationen müssen gem. Archivgesetz bzw. Archivverordnung dem Bundesarchiv zur Archivierung angeboten werden.

2. Datenträger, auf denen INTERN und VERTRAULICH klassifizierte Information gespeichert sind, müssen gemäss den Regelungen der Informationsschutzverordnung vernichtet werden.
3. Datenträger, auf denen besonders schützenswerte Personendaten und/oder Persönlichkeitsprofile gespeichert sind, müssen gemäss den Vorgaben von Datenschutzgesetz bzw. Datenschutzverordnung vernichtet werden.
4. Portöffnungen
5. DNS-Einträge
6. Schnittstellen zu anderen Anwendungen
7. Deprovisionierung Service-Identitäten/Autorisierungen
8. Softwarekomponente auf anderen Systemen/Umgebungen

# 10 Abkürzungen

### Definitionen, Akronyme und Abkürzungen

| Begriff / Abkürzung | Bedeutung |
|---|---|
| **AV** | Anwendungsverantwortlicher |
| **BVTax** | Business Valuation Tax |
| **CyRV** | Cyberrisikenverordnung |
| **DSG** | Eidgenössisches Datenschutzgesetz |
| **DSV** | Datenschutzverordnung (Verordnung über den Datenschutz) |
| **DSBO** | Datenschutzbeauftragter der Organisationeinheit |
| **EDÖB** | Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter |
| **eIAM** | IKT-Standarddienst Identitäts- und Zugangsverwaltung (IAM-Bund) |
| **EWS** | eWertschriften |
| **EWV** | Systemverbund elektronisches Wertschriftenverzeichnis |
| **IAMV** | Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes |
| **ICTax** | Income & Capital Taxes |
| **ISBO** | Informatiksicherheitsbeauftragter der Organisationeinheit |
| **ISBD** | Informatiksicherheitsbeauftragter des Departements |
| **ISDS-Konzept** | Informationssicherheits- und Datenschutzkonzept |
| **ISDS-V** | Informationssicherheits- und Datenschutzverantwortlicher im Rahmen des Projekts, gemäss HERMES |
| **ISG** | Informationssicherheitsgesetz (Bundesgesetz über die Informationssicherheit beim Bund) |
| **ISV** | Informationssicherheitsverordnung (Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee) |
| **JP** | Juristische Personen |
| **LE** | Leistungserbringer (BIT für die Betriebs-Infrastruktur, emineo AG für die Anwendung BVTax) |
| **LB** | Leistungsbezüger (Benutzer aus den kant. Steuerverwaltungen mit der SSK als Auftraggeber und dem Delegierten des SSK-Ressorts Informatik als Vertreter der Benutzer) |
| **PL** | Projektleiter |

| | |
|---|---|
| **RHOS** | Red Hat OpenShift[6] |
| **RINA** | Risikomanagementmethode zur Reduktion nachrichtendienstlicher Ausspähung |
| **Schuban** | Schutzbedarfsanalyse |
| **SLA** | Service Level Agreement |
| **SOAP** | Simple Object Access Protocol |
| **SSK** | Schweizerische Steuerkonferenz |
| **SV** | Systemverantwortlicher |
| **VBNIB** | Verordnung über die Bearbeitung von Personendaten und Daten juristischer Personen bei der Nutzung der elektronischen Infrastruktur des Bundes |

# 11 Anhang

| Identifikator | Titel |
|---|---|
| GRUNDSCHUTZ | Überprüfung der IKT-Grundschutz Umsetzung Version 1.0 vom 28.12.2020 |
| RISIKOANALYSE | ISDS Konzept, Risikoanalyse, Version 1.0 vom 28.12.2020 |
| SCHUBAN | BVTax Schutzbedarfsanalyse, Version 1.0 vom 28.12.2020 |
| BVTax-Architektur | SSK-Atamira-BVTax_CFAE_ArchSkizze_v0.3.vsd vom 16.09.2020. |

**Tabelle 10: Anhänge zum ISDS-Konzept**

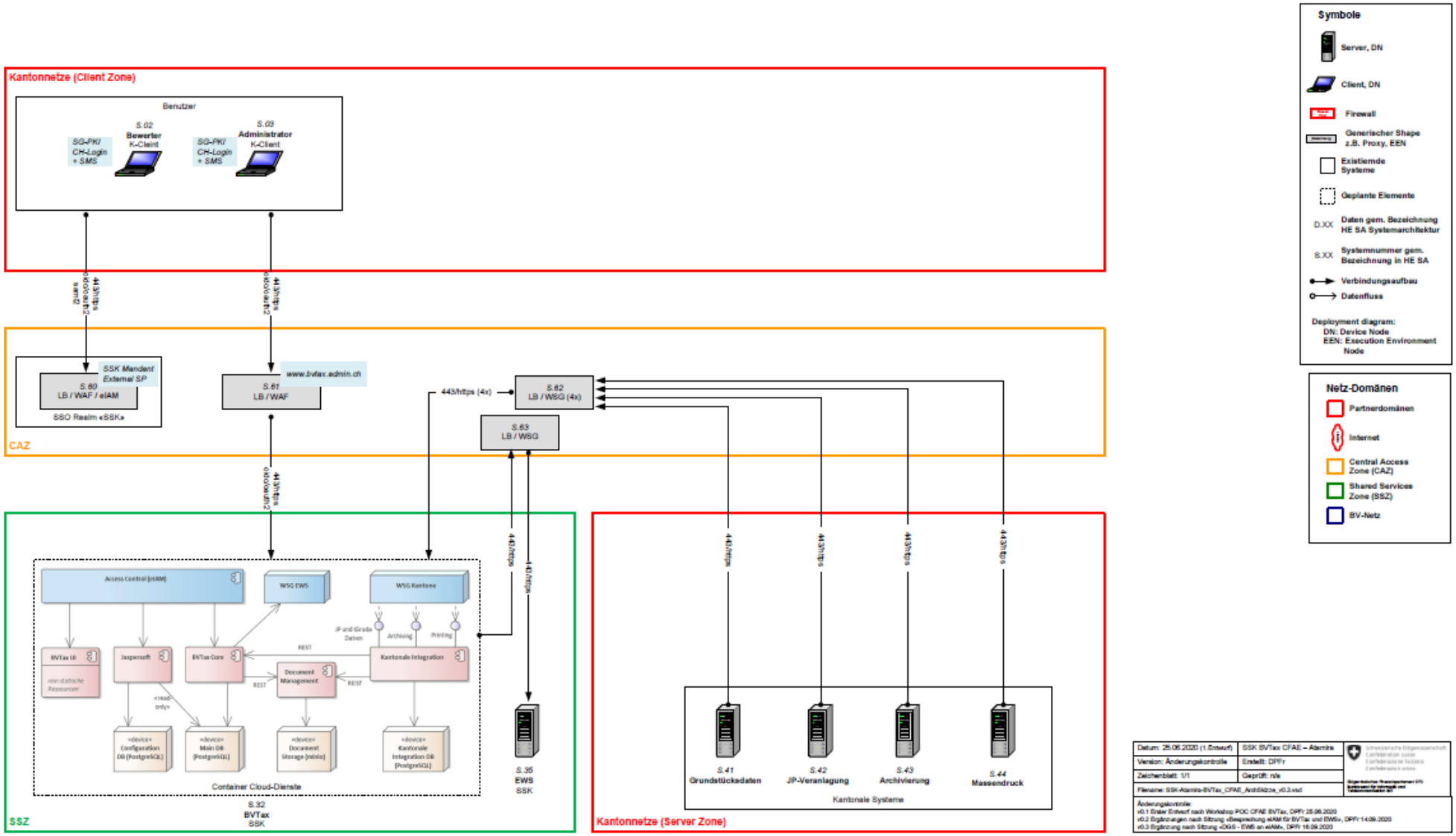
Die Dokumente GRUNDSCHUTZ, RISIKOANALYSE und SCHUBAN liegen als Beilagen vor.

[6] Vgl. https://de.wikipedia.org/wiki/OpenShift

Projektname: BVTax

Schweizerische Steuerkonferenz
Conférence suisse des impôts
Conferenza svizzera delle imposte

# BIT BVTax Architektur




| | |
|---|---|
| Datum: 25.06.2020 (1.Entwurf) | SSK BVTax CFAE – Alamira |
| Version: Änderungskontrolle | Erstellt: DPFr |
| Zeichenblatt: 1/1 | Geprüft: n/a |
| Filename: SSK-Alamira-BVTax_CFAE_Architektur_v0.3.vsd | |

Änderungskontrolle:
v0.1 Erster Entwurf nach Workshop POC CFAE BVTax, DPFr 25.06.2020
v0.2 Ergänzungen nach Sitzung «Besprechung eIAM für BVTax und EWS», DPFr 14.09.2020
v0.3 Ergänzung nach Sitzung «DGS - EWS an eIAM», DPFr 16.09.2020