Schweizerische Steuerkonferenz
Conférence suisse des impôts
Conferenza svizzera delle imposte

Wenn ausgefüllt mindestens: INTERN

Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept)

eWertschriften EWS

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	30.09.2020	Einpflegen Review-Befunde	Bruno Buess
1.0	28.12.2020	Abnahme Atamira PA - 15.10.2020	Bruno Buess
1.1	29.11.2021	Ergänzungen Kap.4 und Kap. 5.3	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

Abbildungen

Tabellenverzeichnis

Anhang

BIT EWS-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	Der Anschluss privater mobiler Geräte an das Bundesnetzwerk ist verboten. Davon ausgenommen ist der Anschluss an die Public Wireless- und Webmail-dienste der LE sowie andere im Standarddienst Datenkommunikation geregelte Netzwerkzugänge.	Der Einsatz von mobilen Geräten ist für EWS nicht vorgesehen. Sollte der Einsatz von (privaten) Tablets zugelassen werden, dann erfolgt der Zugang über eIAM mit 2 Faktor Authentisierung via SMS-Code.
7.1.1	Zwei-Wege-Authentifizierung Erfolgt die Anmeldung bei erhöhtem Schutzbedarf (gem. Schutzbedarfsanalyse) mittels einer 2-Faktor Authentisierung (z. B. Einsatz von Zertifikaten)?	Mit der eIAM-Integration wird sichergestellt, dass die Authentifizierung den Vorgaben entspricht.

9.2	Mitarbeitende mit administrativen Privilegien müssen sich an den Systemen mittels Zwei-Faktor-Authentifizierung anmelden. Kann dies technisch nicht gewährleistet werden, sind die Umgebungen vom übrigen BV-Netz zu trennen.	Mit der eIAM-Integration wird sichergestellt, dass die Authentifizierung den Vorgaben entspricht.
8.2 8.3 8.4 12.1.3 16.1	Ein Organisationshandbuch muss vor Inbetriebnahme fertiggestellt und freigegeben werden.	Das Organisationshandbuch (OHB) muss für EWS unter Mitwirkung von LE (BIT und GFT Schweiz AG) und LB erstellt und vom Auftraggeber freigegeben werden.
7.1.9 13.1.7	Datenzugriffe auf EWS dürfen nur verschlüsselt erfolgen. Die Daten sind bei der Übertragung zu verschlüsseln.,.	Alle Zugriffe erfolgen verschlüsselt mit HTTPS und SSL/TLS (TLS 1.2) *Hinweis:* Aufgrund einer Sicherheitslücke dürfte das BIT auf TLS 1.3 umstellen
14.2.1	Testdaten sind entsprechend ihrer Einstufung zu schützen. Ist es unumgänglich, dass produktive Daten zu Testzwecken verwendet werden, sind diese gemäss ihrer Einstufung zu schützen.	Ist durch die LE (BIT und GFT Schweiz AG) technisch und organisatorisch sichergestellt. Der Standort der Entwicklungs- und Testumgebung (Server und Datenbanken) in der Schweiz ist sicherzustellen.
	Aus der Risikoanalyse:	
R1 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 GFT Schweiz AG) 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 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 Ausweitung der Betriebszeiten auf 7x24h ist sichergestellt.

R6	Betriebsmittel sicherstellen, betrifft auch die Finanzierung für den längerfristigen Betrieb von EWS	Die Finanzierung für den Betrieb von EWS ist für die SSK durch vertragliche Vereinbarungen mit allen Kantonen und der ESTV für einen längerfristigen Zeithorizont sichergestellt
Generell	Umsetzung der Massnahmen Sind alle Massnahmen aus der Risikoanalyse des ISDS-Konzeptes umgesetzt? Sind die Restrisiken dem Kunden mitgeteilt worden?	Die Restrisiken sind dem Kunden mitgeteilt worden. Die Massnahmen aus der Risikoanalyse sind noch umzusetzen.
	Aus dem ISDS-Konzept	
	Datenbearbeitungsreglement	Mit EWS werden bei der Aktionärsregistrierung Personendaten verarbeitet. Es ist ein Datenbearbeitungsreglement zu erstellen, da verschiedene kantonale Steuerbehörden mit EWS arbeiten und Schnittstellen zu kantonalen und ESTV-Systemen bestehen.
	Anmeldung der Datensammlung beim EDÖB	Da mit EWS 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: Matthias Schwaller, 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	EWS-Schutzbedarfsanalyse, Version 1.1 vom 19.11.2021
GRUNDSCHUTZ	Überprüfung der IKT-Grundschutz Umsetzung, Version 1.1 vom 19.11.2021
RISIKO-ANALYSE	ISDS Konzept, Risikoanalyse, Version 1.1 vom 19.11.2021

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 Erhöhte Anforderungen an die Schutzwürdigkeit (nicht DSG/ISV relevant)	Es werden keine besonders schützenswerte Personendaten verwendet. Es werden Daten verarbeitet die Amts- und Steuergeheimnisse darstellen (Art. 320 StGB) 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 anonymisiert 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. Die folgenden Erweiterungen wurden 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. Als Aktionärs-ID wird die AHVN13 verwendet und dazu auch Ort und Land gespeichert. - Die Webservice Benutzerzugriffe erfolgen über das Web-Service-Gateway (WSG) mittels Klasse C-Zertifikate. Alle Daten können nur in der eigenen (kantonalen) Domäne abgefragt werden.
Verfügbarkeit Max. zulässige Ausfalldauer?	Dies ist mit den LE (BIT und GFT Schweiz AG) im Rahmen des SLA vereinbart.

Sicherheitsaspekt	Beschreibung
Integrität Spezielle Anforderungen	Alle Daten müssen korrekt und nachvollziehbar sein.
Nachvollziehbarkeit 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 EWS 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** 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** 1. Bereits die Ausschreibung ist sensitiv[3]: Bekanntgabe der geplanten Beschaffung ist bereits risikorelevant; Bekanntgabe der technischen Spezifikationen in der Ausschreibung ist bereits risikorelevant. 2. Outsourcing von Dienstleistungen, wo sensitive Daten faktisch und

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

	unumgänglich die Systeme der Bundesverwaltung verlassen (Betrieb/Support, Wartung): • Managed Services (Risiko durch Verlust der Vertraulichkeit, Integrität und Nach-vollziehbarkeit): Daten werden externen IKT-Anbietern zur weiteren Verarbeitung/Operationalisierung übergeben; • Managed Services (Risiko aufgrund der Beeinträchtigung der Verfügbarkeit durch nachrichtendienstliche Tätigkeit): Operationalisierungen/Prozesse/Dienstleistungen werden integral nach aussen gegeben. 3. Betriebsleistungen sowie Auf- und Abbauleistungen an internen kritischen Infrastrukturen mit autorisiertem Zugang zur zentralen Infrastruktur oder zu Applikationen: • Remote Inbetriebnahme mit Zugang zu Daten bzw. zum zentralen Management-system der Infrastruktur bzw. Applikation; • Remote Wartung oder Support mit Zugang zu Daten bzw. zum zentralen Managementsystem der Infrastruktur/Applikation, inklusive die Möglichkeit, Daten weg zu kopieren; • On-Site Inbetriebnahme mit Zugang zu Daten bzw. zum zentralen Managementsystem der Infrastruktur/Applikation; • On-Site Wartung oder Support mit Zugang zu Daten bzw. zum zentralen Managementsystem der Infrastruktur/Applikation. • Bei diesem Kriterium sind auch die Aspekte betreffend möglicher Amtsgeheimnis-verletzung zu prüfen. 4. Beschaffung spezifischer besonders sensitiver IKT Infrastrukturen, vor allem für: • Firewall, IPS (Intrusion Prevention System), IDS (Intrusion Detection System), Ap-plication Control, Anti-bot, Antivirus, Identity Awareness; • Verschlüsselungsinfrastruktur inklusive Entwicklung, Support, Wartung, Audits mit Zugriff auf Kernapplikationen und vertrauliche Daten/Infos; • IAM (Identity and Access Management)-Infrastruktur sofern korrumpierender Zu-griff auf Applikationen, Daten und Informationen möglich. 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** 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.

EWS hat zwar gegenseitige Abhängigkeiten zu kantonalen IKT Infrastrukturen, aber es sind keine direkten Zugriffe aus EWS auf kantonale Systeme möglich. Aus diesem Grund ist eine erhebliche Gefährdung der kantonalen IKT-Infrastrukturen auszuschliessen.
Mit EWS werden auch keine schützenswerte 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	Christian Holzreiter, GFT Schweiz 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

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.

Die folgenden Erweiterungen wurden 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.

5.4 Beschreibung der zu bearbeitenden Daten

In der Anwendung EWS werden die folgenden Daten bearbeitet:

- Stammdaten zu kotierten und nicht kotierten Gesellschaften
- Stammdaten zu kotierten und nicht kotierten Titeln
- Stammdaten zu nicht kotierten ausländischen Unternehmen
- Stammdaten zu nicht kotierten ausländischen Titeln
- Ereignisse und Erträge zu kotierten und nicht kotierten Titeln
- Bewertungen von nicht kotierten Unternehmen
- Steuerwerte zu nicht kotierten Unternehmen
- Aktionäre und Beteiligungen bei Immobiliengesellschaften
- Daten zur wirtschaftlichen Handänderung
- Benutzer, Rollen und Berechtigungen

Für EWS 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 EWS Personendaten bearbeitet werden, muss die Datensammlung beim EDÖB angemeldet werden.

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

5.5 Architekturskizze / Systemübersicht

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

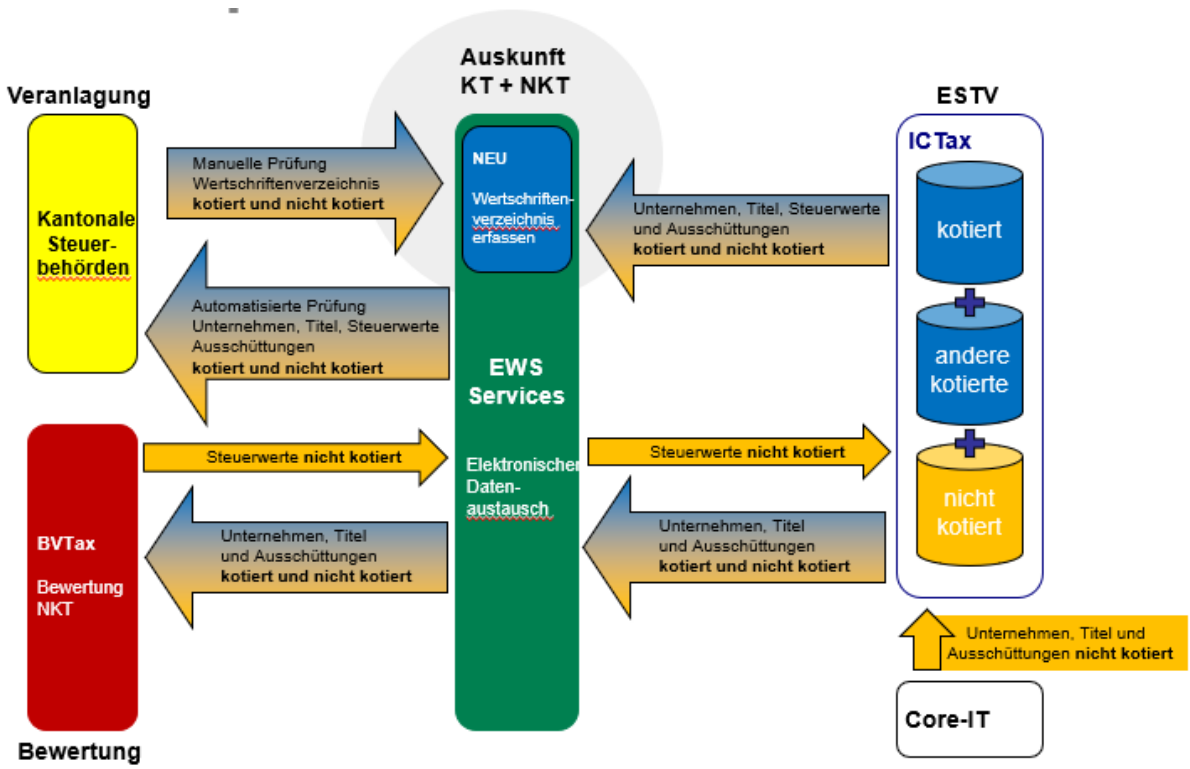


Abbildung 1: Systemübersicht EWS mit Schnittstellen zu Umsystemen

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

5.6 Beschreibung der zugrundeliegenden Technik

Die Systemarchitektur zu EWS mit den verwendeten Komponenten ist in den Betriebshandbüchern BHB beschrieben. Diese sind unterteilt in:

- EWS Betriebshandbuch Vol 1 Allgemein.docx
- EWS Betriebshandbuch Vol 2 Server.docx

Die Dokumente sind veraltet und werden bis Ende 2023 entsprechend aktualisiert.

5.7 Rollen und Berechtigungen

Die Rollen und Berechtigungen sind im EWS Organisationshandbuch beschrieben.
Die Webservice Benutzerzugriffe auf EWS erfolgen über das Web-Service-Gatewav (WSG) mittels Klasse C-Zertifikate.

Für die manuellen Auskunft erfolgen sämtliche Benutzerzugriffe auf EWS 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. Mit der Erweiterung wird es eine Benutzerverwaltung mit mindestens drei Rollen Gast, Auskunft und Administrator geben.

Benutzer werden nach einer Inaktivität von 60 Tagen im System automatisch gelöscht.

Die Details werden in einer Spezifikation noch definiert.

6 Risikoanalyse und Schutzmassnahmen

6.1 Restrisiken

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

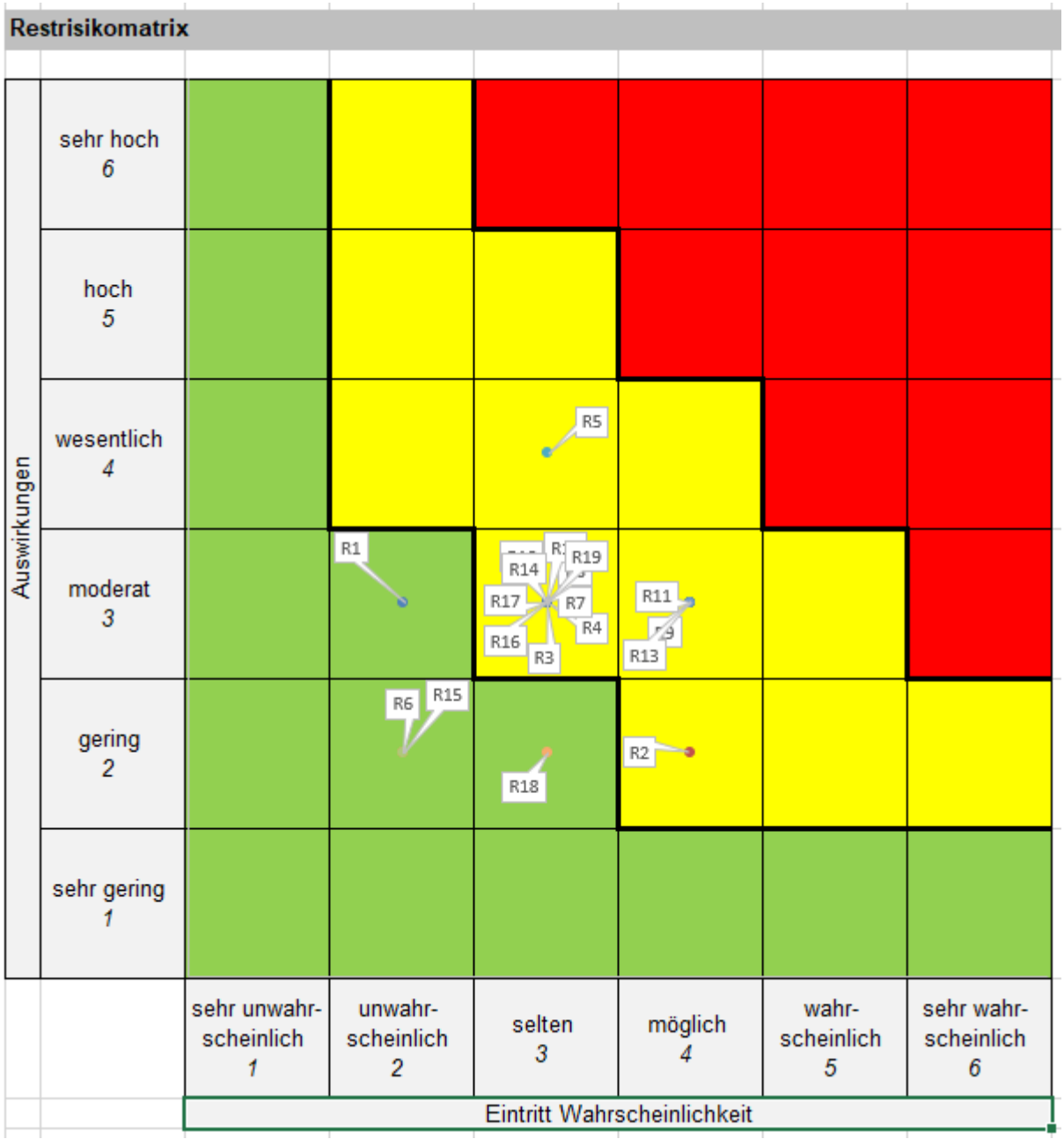


Abbildung 2: Restrisikomatrix aus EWS-ISDS-Sicherheitsanalyse

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 EWS 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. Für den Zugriff auf diese administrative Managementebene bzw. auf die zu administrierenden Zielsysteme ist eine 2-Faktor-Authentifizierung umzusetzen.	Die EWS Serversysteme sind nur durch berechtigte Administratoren aus dem BIT erreichbar. Mit der eIAM-Integration wird sichergestellt, dass die Authentifizierung den Vorgaben entspricht.
8.2 8.3 8.4 12.1.3 16.1	Ein Organisationshandbuch muss vor Inbetriebnahme fertiggestellt und freigegeben werden.	Das Organisationshandbuch (OHB) muss für EWS unter Mitwirkung von LE (BIT und GFT Schweiz AG) und LB erstellt und vom Auftraggeber freigegeben werden.
7.1.9 13.1.7	Datenzugriffe auf EWS dürfen nur verschlüsselt erfolgen. Die Daten sind bei der Übertragung zu verschlüsseln.,.	Alle Zugriffe erfolgen verschlüsselt mit HTTPS und SSL/TLS (TLS 1.2) *Hinweis:* Aufgrund einer Sicherheitslücke dürfte das BIT auf TLS 1.3 umstellen
14.2.1	Testdaten sind entsprechend ihrer Einstufung zu schützen. Ist es unumgänglich, dass produktive Daten zu Testzwecken verwendet werden, sind diese gemäss ihrer Einstufung zu schützen.	Ist durch die LE (BIT und GFT Schweiz AG) technisch und organisatorisch sichergestellt. Der Standort der Entwicklungs- und Testumgebung (Server und Datenbanken) in der Schweiz ist sicherzustellen.

Tabelle 4: 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 *Massnahme:* Die Systeme sind laufend zu überwachen (Monitoring)
R3	Ausfall oder Störung von Dienstleistern	Schlüsselpersonen nicht verfügbar *Massnahme:* Stellvertretung und Knowhow Sicherung und Zugang ist sicherzustellen
R4	Ausspähen von Informationen, Spionage, Abhören	Ungenügend vor unerlaubtem Zugriff geschützt *Massnahme:* 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 *Massnahme:* Daten sind zu verschlüsseln und bei Ereignissen gilt der definierte Incident-Prozess
R7	Manipulation von Informationen, Hard- oder Software	Fahrlässigkeit, unbeabsichtigte Beschädigung durch Administratoren *Massnahme:* Risikominderung durch definierte Prozessablaufe und kontrollierte Einhaltung.
R8	Zerstörung, Ausfall oder Fehlfunktion von Geräten oder Systemen	Fahrlässigkeit, unbeabsichtigte Beschädigung durch Administratoren *Massnahme:* Mit entsprechenden Massnahmen (Monitoring, etc.) kann das Risiko vermindert werden.
R9	Softwareschwachstelle oder -Fehler	nicht Patchen des Systems, Fehlerhafte Releases, fehlerhafte Patches (ungenügendes Testing) *Massnahme:* Mit Wartungsverträgen sind die Reaktions- und Fehlerbehebungszeiten definiert
R10	Verstoss gegen Vorschriften oder Regelungen	Nicht Einhaltung der Vorgaben und Prozesse, mangelnde Schulung *Massnahme:* 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	Verletzung der Integrität und Datenschutz *Massnahme:* Der Zugang ist nur auf berechtigte Benutzer be-

	Berechtigungen	schränkt und erfolgt über eIAM mit 2-FA. Die Systeme sind laufend zu überwachen (Monitoring)
R12	Personalausfall	Schlüsselpersonen nicht verfügbar *Massnahme:* 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 *Massnahme:* Risikominderung durch eIAM mit 2FA und durch aktives Monitoring.
R14	Verhinderung von Diensten (Denial of Service), Sabotage	Insider Angriff *Massnahme:* Die Systeme sind laufend zu überwachen (Monitoring)
R16	Datenverlust	Ungenügend getestetes Backup/Restore *Massnahme:* Die Backup-/Restoreprozesse sind periodisch zu testen
R17	Informationsabfluss über Umsysteme	Backup ist nicht Verschlüsselt, unkontrollierte Datenexporte durch Entwicklung und Support *Massnahme:* Mit organisatorischen Massnahmen kann dieses Risiko minimiert werden. Die Systeme sind laufend zu überwachen (Monitoring)
R19	Ausfall der Umsysteme / Basisinfrastruktur	Ausfall der Basissysteme *Massnahme:* Die Systeme sind laufend zu überwachen (Monitoring)

Tabelle 5: 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 EWS 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		Organisationshandbuch und Schulung
5	Ausreichende Ressourcen für den IT-Betrieb EWS	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		
11	Kryptografische Sicherung vertraulicher Daten	LE	
12	Verwenden von qualitativ guten Passwörtern. Einhaltung der Passwortregeln	LE	

Tabelle 6: Massnahmenliste

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

6.3 Potenzielle sicherheitsrelevante Vorfälle

Die Anwendung EWS 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.

Vorfall	Kriterien
Massiver Download / Export	Derselbe Benutzer greift in einem kurzen Zeitraum auf viele Dokumente verschiedener Geschäfte zu
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 7: Liste der möglichen Sicherheitsrelevanter Vorfälle

7 Wiederherstellung des Geschäftsbetriebes

Gemäss Einschätzung des PL-LB ist für EWS 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 EWS.

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 Korrek-

turmassnahmen 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 Anwendungsverantwortliche 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 EWS	LE	Die Zeitspanne eines umfangreichen Disaster Recovery variiert von - 3-5 Stunden (falls nur EWS betroffen ist) bis - 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 8: 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 EWS 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[5]
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 1.1 vom 19.11.2021
RISIKOANALYSE	ISDS Konzept, Risikoanalyse, Version 1.1 vom 19.11.2021
SCHUBAN	EWS Schutzbedarfsanalyse, Version 1.1 vom 19.11.2021
EWS Architektur	BIT SSK-EWS_ArchSkizze_v0.9b.vsd vom 01.10.2020.

Tabelle 9: Anhänge zum ISDS-Konzept

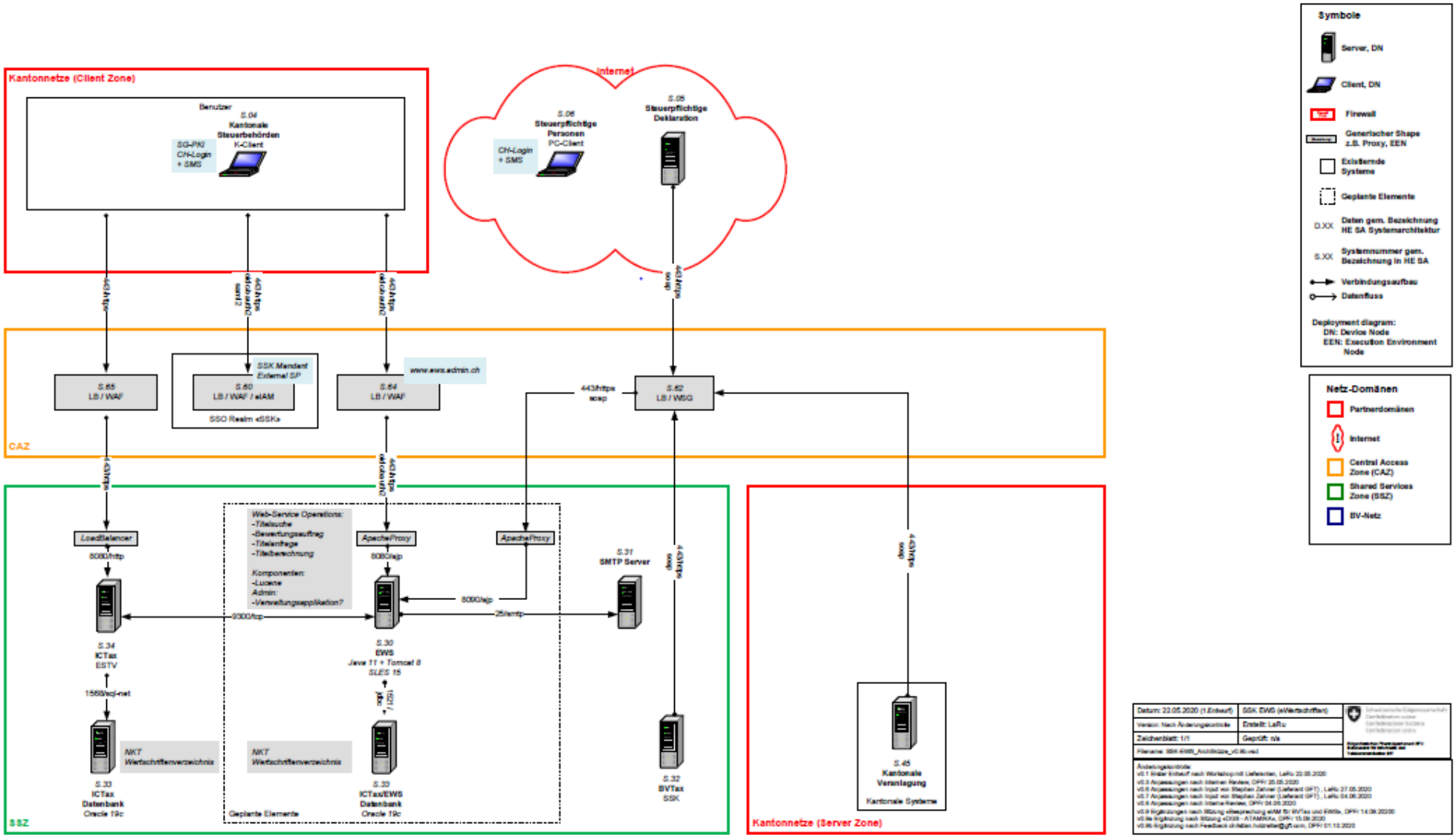
Die Dokumente GRUNDSCHUTZ, RISIKOANALYSE und SCHUBAN liegen als Beilagen vor.

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

Projektname: eWertschriften EWS

Schweizerische Steuerkonferenz
Conférence suisse des impôts
Conferenza svizzera delle imposte

BIT EWS-Architektur



Datum: 22.05.2020 (1.Entwurf)	SSK EWS (eWertschriften)
Version: Nach Änderungskontrolle	Erstellt: LaRu
Zeichenblatt: 1/1	Geprüft: n/a
Filename: SSK-EWS_Architektur_v0.90.vsd	

Änderungskontrolle:
v0.1 Erster Entwurf nach Workshop mit Lieferanten, LaRu 22.05.2020
v0.3 Anpassungen nach Interner Review, DPH 25.05.2020
v0.6 Anpassungen nach Input von Stephan Zahner (Lieferant GFT) , LaRu 27.05.2020
v0.7 Anpassungen nach Input von Stephan Zahner (Lieferant GFT) , LaRu 04.06.2020
v0.8 Anpassungen nach interne Review, DPH 04.06.2020
v0.9 Ergänzungen nach Sitzung eNewsprechung eIAM für BVTax und EWSs, DPH 14.06.2020
v0.9a Ergänzung nach Sitzung vDDS - ATAMKKa, DPH 15.06.2020
v0.90 Ergänzung nach Feedback christian.hubmeier@gft.com, DPH 01.10.2020