ISS System-Audit

April 2013

Datum 16.04.2013
Dok.
Version 1.0

Zühlke Engineering AG
Aarbergergasse 29
3011 Bern
Schweiz

Telefon+41 31 313 0911
Telefax +41 31 313 0912

info@zuehlke.com
zuehlke.com

Änderungsnachweis

Datum	Version	Verfasser	Änderung
11.03.2013 bis 5.4.2013	0.1 bis 0.8.5	Auditoren	Einarbeitung der Ergebnisse des Szenarien-WS Einarbeitung Workshop Hersteller Einarbeitung Workshop ISC-EJPD Einarbeitung Workshop mit Testmanager Ergänzung Umfeld und Anforderungen Bewertung hinsichtlich Zielen und Fragestellungen Erkenntnisse und Empfehlungen
5.4.2013	0.9	Auditoren	Finalisierung des ersten Drafts für internen Review und Rückmeldung an EJPD.
08.4.2013 bis 16.4.2013	1.0	Auditoren	Finalisierung des Dokumentes: Verschlankung des Dokumentes und Schärfung des Management Summary

Inhaltsverzeichnis

Abbildungsverzeichnis

Referenzen

Id	Name des Dokuments	Autor	Datum	Version
1	Pflichtenheft Interception System Schweiz (ISS)	Kernteam des Projekts ISS	15.03.2010	1.0
2	Funktionsliste: Anhang zum und damit Bestandteil des Pflichtenhefts	Kernteam des Projekts ISS	15.03.2010	
3	Specification – Fault Tolerance concept – CS	Hersteller	25.01.2013	1.3.1
4	Specification – Fault Tolerance concept – PS	Hersteller	26.02.2013	1.3.0
5	Sicherheitsweisung ISC-EJPD Nr. 10	ISBO ISC-EJPF	23.03.2010	n.v.
6	Weisungen des IRB über die Informatiksicherheit in der Bundesverwaltung (WIsB), SR 172.010.58	Informatikrat des Bundes (IRB)	01.11.2004	1.11.2007
7	System Requirement Guide For ISS Integration and Production Systems	Hersteller	07.02.2011	1.2.0
8	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)	Bundesrat	6.10.2000	1.1.2011
9	Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)	Bundesrat	31.10.2001	1.1.2012
10	Antrag ans ADB zum Einsatz der Antiviren-SW im ISS-System	TPL ISS	27.02.2013	1.60
11	Beschlussprotokoll der 68. ABD Sitzung – 05. März 2013	ADB	05.03.2013	1.0

1. Management-Zusammenfassung

Mit dem Projekt „Interception System Schweiz" (ISS) wird die zentrale Informatik-Infrastruktur des Dienstes ÜPF erneuert. Das Projekt ISS wurde unter Einbezug aller an einer Überwachungsmassnahme Beteiligten – Konferenz der kantonalen Justiz- und Polizeidirektoren, Konferenz der StrafB der Schweiz, Bundesanwaltschaft, Bundeskriminalpolizei, Schweizerischer Verband der Telekommunikation – im August 2008 initiiert und sollte im Sommer 2011 den produktiven Betrieb aufnehmen.

Gemäss ISC-EJPD waren der Lieferant und der Hersteller bisher nicht in der Lage, ein System zu liefern, das bezüglich Stabilität und Performance den Anforderungen an einen produktiven Betrieb genügen würde. Das Projekt gerät immer mehr in Zeitverzug und gesetzlich vorgesehene neue Funktionalitäten werden nicht termingerecht ausgeliefert werden können. Gleichzeitig ist die Lebensdauer des aktuellen „Alt-Systems" begrenzt.

Zur Klärung des Status-Quo wurde Zühlke mit der Durchführung eines System-Audits beauftragt. Der System-Audit hat zum Ziel die zentrale Leitfrage „Ist der Hersteller in der Lage, ein lauffähiges System zu liefern?" zu klären. Die Durchführung des System-Audit ist bezüglich Zeit und Umfang sehr anspruchsvoll. Der methodische Ansatz basierte auf der Befragung der Bereiche Projektmanagement, Business Anforderungen, Architektur, Applikation, Betrieb und Schulung. Befragt wurden der Hersteller, der Betrieb des ISC-EJPD und die notwendigen Stakeholder. Zühlke bedankt sich besonders bei allen Beteiligten für die Beantwortung der Fragen. Der Bericht des System-Audits ist eine Bestandsaufnahme und erhebt keinen Anspruch auf Vollständigkeit.

1.1 Bewertung der Anforderungen

In einem Systemaudit wird geprüft, ob das System die Anforderungen erfüllt. Die Grundlage des Vertrags war das Pflichtenheft [1] mit Funktionsliste [2]. Diese Anforderungen sind auf einer sehr hohen Abstraktionsebene beschreiben und nicht widerspruchsfrei. Sie wurden im Projektverlauf nur teilweise geschärft, die entsprechenden Änderungen aber nicht nachdokumentiert. Daher ist es für die Auditoren unmöglich den zum aktuellen Zeitpunkt geltenden vollständigen Satz der Anforderungen zu ermitteln. Die Bewertung des Systems bezieht sich daher auf das ursprüngliche Pflichtenheft.

Für den Audit wurden noch weitere zu untersuchende Anforderungen an das System definiert:

- von Seiten StrafB (Fragen 1-7 inklusive Szenarien [Px], [Qx] und [Lx])
- Erweiterte Aufgabenstellung durch das ISC-EJPD

Empfehlung: Umgehende Klärung und Schärfung der noch fehlenden Anforderungen. Priorisierung der von den StrafB benötigten Funktionalitäten.

Wichtiger Hinweis zur Begriffsverwendung

- **Rückwirkende Überwachung:** Die bei den FDAs gespeicherten Daten werden aktuell per Datenträger direkt an die StrafB übermittelt. Aus technischer Sicht des ISS sind solche Anforderungen (bis auf die Auftragsabwicklung im WMS) nicht im Scope.
- **Echtzeit-Überwachung:** Daten werden direkt von den FDAs an das ISS ausgeleitet, vom ISS empfangen und gespeichert. Die Auswertung der Daten durch die StrafB kann **LIVE** (im Sinne von Mithören) oder **nachträglich** erfolgen.

Der Begriff „Echtzeit-Überwachung" muss daher vom Begriff der „Live-Beobachtung" (oder LIVE) im Sinne eines Mithören des Gesprächs unterschieden werden. Die Begriffe sind in den Anforderungen nicht immer korrekt getrennt.

1.2 High-Level-Bewertung des Systems:

Die überwiegende Mehrheit der Anforderungen aus der Funktionsliste [2] an das ISS-System wird vom Hersteller bereits im Standard unterstützt. Es gab Erweiterungen dieses Standards zur Ergänzung einzelner Funktionalitäten. Vor allem im Bereich WMS, welches nicht Bestandteil des Audits war, gab es Individualentwicklungen.

Das Projekt ISS hat die Ablösung von zwei Systemen zum Ziel. Beide Teilsysteme haben aktuell einen unterschiedlichen Entwicklungsstand. Wir empfehlen daher (wie auch ursprünglich geplant) eine gestaffelte Einführung.

1.2.1 CS (Ablösung von System A)

- Die Kernfunktionalitäten für CS sind gegeben.
- Es gibt noch einige Fehler im System (vor allem bei der Live-Beobachtung). Diese werden vom Hersteller aktuell behoben.

Empfehlung:

- Pilotierung und sorgfältiger Gesamttest
- bei Erfolg Einführung des Systems

1.2.2 PS (Ablösung von System B)

Die Anforderungen sind hier deutlich unvollständiger als bei CS, da dieser Umfang nachträglich hinzugefügt und nur sehr wenig abgeklärt wurde. Es gibt noch einige kritische widersprüchliche Anforderungen, welche dringend geklärt werden müssen (Virenscanner, Verfügbarkeit).
Das System erfüllt die aktuell geforderte Echtzeitüberwachung von 25 Mbit/s. Der Durchsatz pro Target ist im Pflichtenheft nicht spezifiziert.
Kritische Punkte in der Architektur sind:

- Das Redundanz- und Verfügbarkeitskonzept ist bis heute nicht verabschiedet worden und deren Umsetzung ausstehend. Die genauen Anforderungen sind dringend zu klären, um das Konzept verabschieden zu können.
- Die Architektur ist optimiert für die Store&Forward-Verarbeitung. Für die LIVE-Beobachtung gibt es einen dedizierten Datenpfad. Der Dekodierungsaufwand ist durch den Investigator zu leisten.

Empfehlung:

- Pilotierung und Test des aktuellen Systems
- Klärung der kritischen Anforderungen
- Fertigstellung der Konzepte für Verfügbarkeit und Redundanz
- Review dieser Konzepte
- Umsetzung bei positivem Review-Ergebnis

1.2.3 Erweiterung des Systems

Im Bereich FMÜ wird es kontinuierlich zu technologischen Anpassungen und funktionalen Erweiterungen kommen. Dies bedingt die ständige Weiterentwicklung des ISS und den kontinuierlichen Ausbau der Hardware- und Software-Komponenten.

- Die aktuelle Architektur besitzt im Bereich Ausleitung und bei der Datenbank Engpässe, welche eine weitere Skalierung des Systems behindern. Um diese zu überwinden, sind Änderungen in der Architektur notwendig.
- Von entscheidender Bedeutung ist die Festlegung des Durchsatzes pro Target.
- Der Hersteller arbeitet bereits an Lösungen, diese liegen allerdings noch nicht vor und konnten daher nicht bewertet werden.

- Im Rahmen dieser Ausbaustufen gibt es auch Möglichkeiten für die proaktive Einflussnahme für funktionale Erweiterungen durch die StrafB.

Empfehlung:

- Erarbeitung eines Zeitplans für die Ausbaustaufen des Systems hinsichtlich des erwarteten zukünftigen Durchsatzes in der Echtzeitüberwachung.
- Enge Abstimmung mit der Roadmap des Herstellers.
- Die Auditoren gehen davon aus, dass es sehr schwer sein wird, diese Schritte bis Ende 2013 umzusetzen.
- Das Risiko, dass die Skalierbarkeit nicht in dem gewünschten Mass erreichbar ist, ist sehr hoch und muss aktiv gemanagt werden.

1.3 Fazit

Der Hersteller war äusserst zuvorkommend und erläuterte die gestellten Fragestellungen stets in der vom Audit-Team erwarteten Tiefe und Breite. Die Auditoren erhielten freien Zugang zu allen gewünschten Informationen und Personen. Der Hersteller hat einen sehr kompetenten Eindruck vermittelt und kennt die generellen Anforderungen und technischen Details eines Fernmeldeüberwachungssystems. Er verfügt über die geforderte Expertise und hat über die Jahre ein Standard-System entwickelt, welches nach Aussage des Herstellers mehr als 50-mal weltweit im Einsatz ist. Die Auditoren sind zur Auffassung gelangt, dass der Hersteller ein lauffähiges System auf Basis des aktuellen Kriterienkataloges liefern kann.

Das System ist auf die persistente Speicherung der zu überwachenden Daten ausgelegt. Alle Daten werden in einer Datenbank gespeichert, zwecks nachfolgender Analyse und Auswertung durch die StrafB. Aufgrund des technologischen Fortschritts (z.B. Bandbreiten) wird die Architektur einem stetigen Wandel unterliegen. Der Hersteller evaluiert aktuell Anpassungen seiner Architektur.

Das ISS ist für einen Einsatz im CH-WAN-Umfeld geeignet und wird zukünftig einer Weiterentwicklung unterliegen.

Dieses Projekt zeichnet sich durch eine hohe Komplexität aus. Die Infrastruktur basiert auf dem Stand der Technik im Bereich Virtualisierung. Die physische Verbindung zwischen der Datenbank und dem Storage mittels iSCSI-Protokoll ist kritisch zu hinterfragen. In vergleichbaren daten-intensiven Anwendungen hat sich der Einsatz von Fiber Channel sehr bewährt, um die Performanz-Anforderungen im IO-Bereich zu sichern. Sollte im Betrieb das IO-Verhalten der Datenbank sich markant verschlechtern, so ist der Einsatz von Fibre Channel unumgänglich.

Das Rechenzentrum des ISC-EJPD hat das notwendige Wissen, den Betrieb sicherzustellen. Es verfügt über eine leistungsfähige Infrastruktur. Die Installation der ISS-Software-Komponenten wird immer stärker durch den Betrieb wahrgenommen. Das Systemmanagement und Monitoring ist für einen Betrieb geeignet. Das Rechenzentrum kann keine Verantwortung für die ausserliegenden Netzwerke (FDAs und BIT) bzgl. Performanz und Qualität wahrnehmen.

Die Performanz und Qualitätsprobleme haben unterschiedliche Ursachen, welche zum Teil nicht mehr nachvollzogen werden können. Wir empfehlen eine Validierung der Performanz in den Systemgrenzen des Rechenzentrums. Insbesondere empfiehlt sich die Einführung von definierten Messpunkten, um die Performanz-Aspekte qualitativ wie auch quantitativ erheben zu können. Qualitätsprobleme im Bereich von Abstürzen und Fehlbedienungen der Anwendungen sind Aufgabe des Herstellers und sind durch den Qualitätsprozess des Herstellers unterstützt. Der Hersteller hat unmissverständlich die Fehlerbehebung zugesichert. Aktuell sind diverse Probleme behoben und nicht mehr reproduzierbar.

Im Bereich Fehlermanagement ist eine enge Zusammenarbeit zwischen den Beteiligten unabdingbar. Wir empfehlen eine direkte Kommunikation zwischen dem ISC-EJPD Betrieb und dem Hersteller zu etablieren.

Das System verfügt seit Beginn über eine LIVE-Funktion, welche das Mithören von Gesprächen ermöglicht. Diese Funktionalität war zu Beginn allerdings nur eingeschränkt verfügbar (beispielsweise konnte nur ein Client das Gespräch mithören) und wurde im Projektverlauf erweitert. Daraus resultierten Fehler (z.B. wiederholter Verbindungsaufbau),

welche vom Hersteller teilweise schon beseitigt wurden oder deren Beseitigung noch ausstehend ist. Das System ist auf die Verarbeitung der Daten und deren verlustfreie Datensicherung ausgelegt.

Für die zukünftige IP-Überwachung empfiehlt Zühlke den Einsatz von dedizierten Komponenten für die unterbruchsfreie, hochverfügbare und sichere Entgegennahme der IP-Pakete, um mit den zukünftigen Bandbreiten skalieren zu können. ISS muss sicherstellen, dass die Pakete im Anschluss in der notwendigen Taktung verarbeitet werden können.

Im Rahmen eines weiteren Ausbaus (z.B. Langzeitarchivierung) bietet ISS datenbankorientierte Schnittstellen an. Standardisierte Web-Schnittstellen müssen stets auf die Datenbankschnittstellen zugreifen, da in ihnen die sicherheitsrelevanten Aspekte hinterlegt sind. Dieser Ansatz garantiert eine hohe Datensicherheit und schützt vor unerlaubtem Zugriff auf die Datenbestände, da keine direkten SQL-Anfragen auf Tabellen des ISS möglich sind.

Rechtskonformität: Die gesichteten Rechtsgrundlagen sind gut erfüllt, zu einigen Themen (z.B. geo-bezogene Echtzeitalarmierung) besteht aktuell jedoch keine Rechtsgrundlage. Einige Aspekte z.B. zur Überwachung mehrerer Targets sind anhand von [1] und [2] nicht beurteilbar, hier müssten die Umsetzungskonzepte, z.B. das Benutzerkonzept, geprüft werden. Eine solche Prüfung ist nicht Gegenstand dieses Audits.

Zühlke empfiehlt auf Basis der Befragten die Einführung des ISS-Systems unter folgenden Rahmenbedingungen:

- Das Anforderungsmanagement aller Beteiligten wird erheblich verbessert und abgestimmt. Ein Lead-Architekt wird im Projekt verankert, welcher die Anforderungen validiert, prüft und mit Entscheidungskompetenzen versehen ist, um Entscheide zu tätigen.
- Die enge Zusammenarbeit zwischen dem Auftraggeber und dem Hersteller wird etabliert und auf eine vertrauensvolle Basis gestellt.
- Weiterhin gilt es vertrauensbildende Massnahmen für alle Stakeholder zu etablieren. Dies setzt voraus, dass alle Stakeholder ein Interesse an der Fortführung des Projektes haben.
- Der Hersteller behebt die erkannten Mängel umgehend und wird eng in den Einführungs-Prozess eingebunden.
- Es sind grundlegende Entscheidungen ausstehend, welche umgehend getroffen werden müssen. Insbesondere handelt es sich um nicht-funktionale Anforderungen, die einen sehr hohen Einfluss auf das ISS haben.
- Rechtliche Verordnungen mit den FDAs werden erlassen, um die Anlieferung der HI2 Daten wohl-definiert zu regeln.
- Nach erfolgreicher Einführung des Systems werden nur noch GA-Releases des Herstellers auf dem produktiven System installiert. Dies sichert eine hohe Verfügbarkeit des ISS und gleichzeitig die Wahrung der qualitativen Aspekte.

Die Auditoren kommen daher zum Schluss, dass das ISS-System die im Pflichtenheft beschriebenen Kern-Funktionen als Standard bietet.

2. Einleitung

2.1 Ausgangslage

2.1.1 Das Projekt ISS

Mit dem Projekt „Interception System Schweiz" (ISS) wird die zentrale Informatik-Infrastruktur des Dienstes ÜPF erneuert. Das Projekt ISS wurde unter Einbezug aller an einer Überwachungsmassnahme Beteiligten – Konferenz der kantonalen Justiz- und Polizeidirektoren, Konferenz der StrafB der Schweiz, Bundesanwaltschaft, Bundeskriminalpolizei, Schweizerischer Verband der Telekommunikation – im August 2008 initiiert und sollte im Sommer 2011 den produktiven Betrieb aufnehmen.

2.1.2 Aktuelle Situation

Gemäss ISC-EJPD waren der Lieferant und der Hersteller bisher nicht in der Lage, ein System zu liefern, das bezüglich Stabilität und Performance den Anforderungen an einen produktiven Betrieb genügen würde. Das Projekt gerät immer mehr in Zeitverzug und gesetzlich vorgesehene neue Funktionalitäten werden nicht termingerecht ausgeliefert werden können. Gleichzeitig ist die Lebensdauer des aktuellen „Alt-Systems" begrenzt.

2.2 Zusammenfassung der Aufgabenstellung des System-Audits

Leitfrage: Ist der Hersteller in der Lage, ein lauffähiges System zu liefern?

Themenscope:

1. Was sind die Unterschiede zwischen einer üblichen SW- und HW-Installation eines Überwachungssystems des Herstellers und der Installation des ISS? (Wurde die empfohlene = recommended Architektur des Lieferanten realisiert: Storage, SAN, DB, CITRIX, Applikation, Virtualisierung)
2. Welche Unterschiede führen zu den auftretenden Performance und Qualitätsproblemen?
    a. Enduser-Szenarien zur Prüfung definieren
    b. Prüfung der Szenarien gegen Pflichtenheft und Jira
    c. Workshop mit Hersteller
3. Ist das System des Herstellers für den Einsatz in CH - WAN Umfeld geeignet (QOS, Terminal Server CITRIX, Response Time)?
4. (gestrichen)
5. Ist das System des Herstellers für Echtzeitüberwachung ausgelegt und ist die LIVE-Funktion in der ursprünglichen Softwarearchitektur vorgesehen?
    a. Enduser-Szenarien zur Prüfung definieren
    b. Prüfung der Szenarien gegen Pflichtenheft und Jira
    c. Workshop mit Hersteller
6. Ist im System genügend Performanz vorhanden, um zukünftige IP-Überwachungen im geforderten Umfang zu realisieren?
    a. Typische und extreme Mengengerüste ermitteln
    b. Workshop mit Hersteller: Skalierung des Systems, Architektur
7. Ist das Rechenzentrum ISC-EJPD mit den Auflagen des Bundes in der Lage, ein hochkomplexes System im Bereich der Kommunikationsüberwachung für die schweizerischen StrafB zu betreiben?

a. Prüfung der Weisungen gegen das Pflichtenheft
b. Umsetzung Betrieb gegen Vorgaben Hersteller

8. Prüfung der Rechtskonformität:
   a. BÜPF / VÜPF: Kann das ISS die gesetzlich vorgeschriebenen Überwachungstypen entgegennehmen und verarbeiten?
   b. Revision BÜPF: Konzepte des Herstellers zu Langzeitspeicherung sowie Import & Export
9. Prüfen des Pflichtenhefts gegen das System: AR- und K-Anforderungen

2.3 Methodik

Der ISS System-Audit wurde gemäss den in der Abbildung 1 dargestellten Themengebieten untersucht.

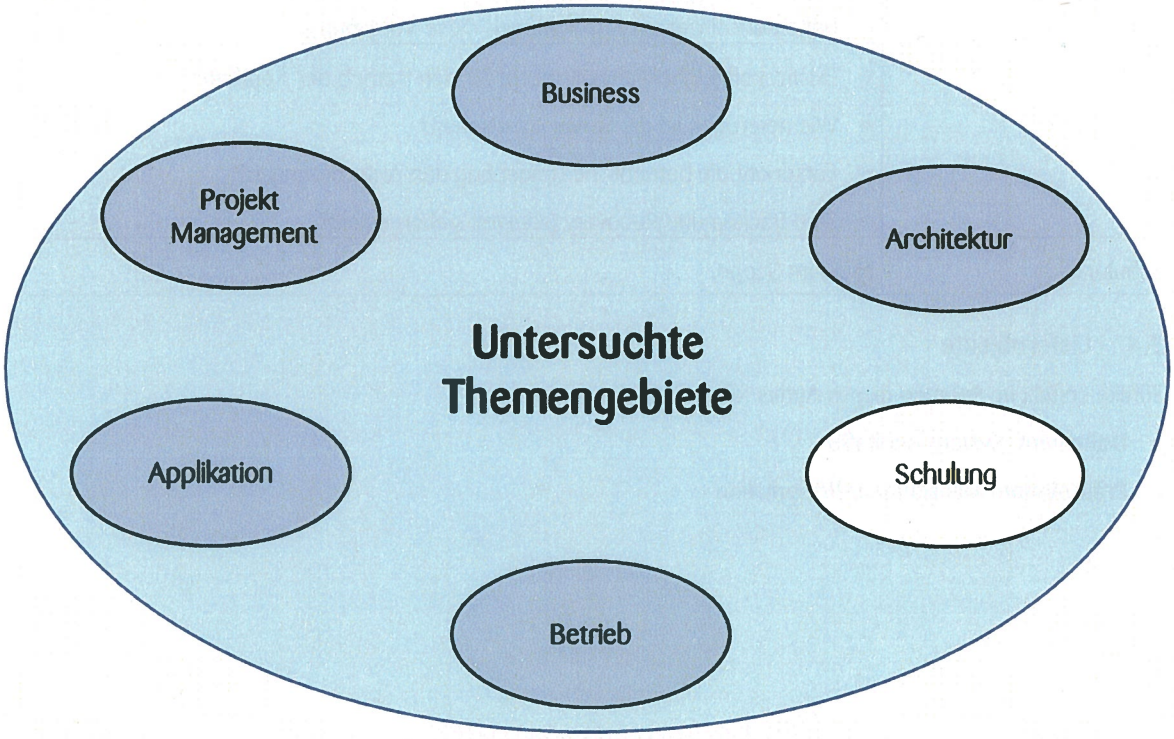

Abbildung 1: Untersuchte Themengebiete

Die einzelnen Themengebiete werden in der folgenden Tabelle präzisiert:

Titel	Beschreibung
Projekt-Management	▪ Besteht ein einheitlicher Projekt-Management-Prozess? ▪ Ist der Prozess geeignet für die Aufgabe? ▪ Ist dieser Prozess dokumentiert? ▪ Wie wird der Prozess gelebt?

Titel	Beschreibung
Business	■ Sind die wichtigsten bestehenden Business-Prozesse erfasst und dokumentiert? ■ Sind die bestehenden Anforderungen (Requirements) erfasst? ■ Sind die neuen Anforderungen erfasst?
Architektur	■ Besteht eine dokumentierte Vision einer System Architektur, die beschreibt wie die einzelnen Applikationen zusammen integriert werden? ■ Ist dieses Konzept geeignet?
Applikation	■ Besteht eine dokumentierte Vorgabe zum Erstellen von Applikationen (z.B. Technologien, Layering, Schnittstellen, Usability-Vorgaben, Coding Guidelines, etc.)? ■ Halten die einzelnen Applikationen diese Vorgaben ein?
Betrieb	■ Existiert ein einheitliches Konzept für den Betrieb der Applikationen? ■ Wie heterogen ist die Server-Landschaft? ■ Entspricht die betriebliche Umgebung den Anforderungen? ■ Sind Backup und Recovery jederzeit sichergestellt?
Schulung	Nicht im Scope.

2.4 Lieferobjekte

Zühlke erstellt im Rahmen dieses Audits folgende Dokumente:

- **Dokument:** System-Audit ISS
- **Präsentation:** Management-Präsentation

3. Übersicht über das Projektumfeld

Das Projekt ISS zeichnet sich durch eine sehr hohe Komplexität bezüglich Anzahl Stakeholder, Kommunikation, Entscheidungswege, Scope (Anforderungen) und Technik aus. Einige Aspekte aus dem Projektumfeld, die zur späteren Bewertung beitragen, sollen daher vorab kurz dargestellt werden.

3.1 Der Dienst ÜPF

Organisatorisch ist der von Gesetzes wegen unabhängige Dienst ÜPF innerhalb des EJPD beim ISC-EJPD angesiedelt.

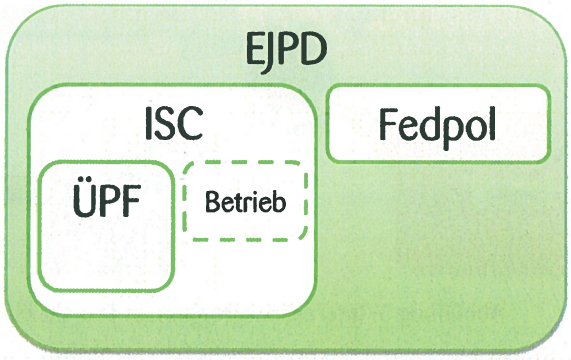

Abbildung 2: Verankerung des Diensts ÜPF im EJPD

Der Werkvertrag mit dem Lieferanten wurde vom Leiter Informatik Service Center (kurz: ISC-EJPD) unterzeichnet und ist damit aus Sicht des Lieferanten der Auftraggeber. Ihm ist der Teilprojektleiter Betrieb des Projekts ISS unterstellt.

Im Projekt-Setup ist der Leiter Dienst Überwachung Post- und Fernmeldeverkehr (kurz: ÜPF) der Auftraggeber des Projekts. Der Leiter ÜPF ist arbeitsrechtlich dem Leiter des ISC-EJPD unterstellt. Ihm obliegt nicht die volle Budget-Kontrolle.

Der Projektleiter wurde von Leiter ISC-EJPD angestellt und rapportiert Projektfortschritte an den Projekt-Auftraggeber.

Gemäss BÜPF (Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs, [8]) stellt der ÜPF zentral allen legitimierten Polizei-Einheiten (Bundes- und Kantonspolizei) ein System zur Fernmeldeüberwachung (kurz: FMÜ) zur Verfügung. Dieses FMÜ-System betreibt das ISC-EJPD in seinem Rechenzentrum.

BÜPF [8] und VÜPF [9] regeln die Aufgaben-Kompetenzen-Verantwortungen (AKV) des ÜPF. Das Verständnis der AKV ist nicht einheitlich bei den involvierten Parteien. Es gibt Strömungen bei den StrafB, die das ÜPF stark einschränken und einige zentrale Kompetenzen den Polizei-Einheiten des Bundes und der Kantone übertragen möchten. Dieses politische Thema belastet das Projekt stark.

3.2 Stakeholder im Projekt ISS

Das Projekt ISS bewegt sich im Spannungsfeld von 4 Hauptgruppen mit diversen Untergruppen.

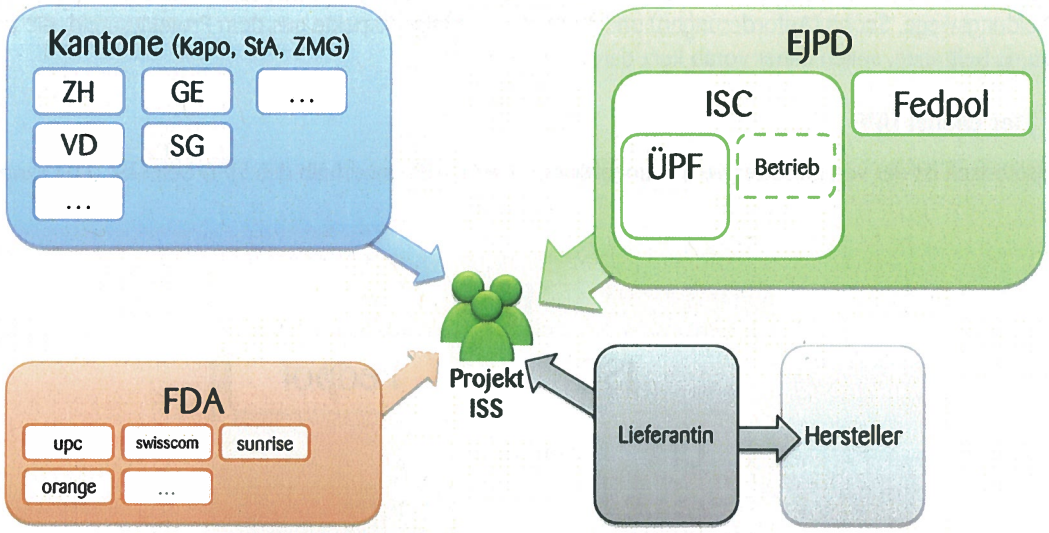

Abbildung 3: Interessensgruppen im Projekt ISS

Da die in Betrieb befindlichen Überwachungssysteme das Ende ihres Lebenszyklus erreicht haben, wurde das Projekt ISS zur Evaluation und Einführung eines neues System unter dem Arbeitstitel „Ablöse LIS" ins Leben gerufen. Die Anforderungen wurden in einem Pflichtenheft [1] und in einer ergänzenden Funktionsliste [2] (beide Teile zusammen kurz „Pflichtenheft" genannt) gebündelt. An der Erarbeitung des Pflichtenhefts waren einige Personen beteiligt, die bereits bei der Einführung des LIS dabei waren. Alle an der Erarbeitung beteiligten Interview-Partner der Gruppen Kantonspolizei und EJPD äussern sich positiv sowohl zum Projekt-Geist als auch zum Ergebnis der Phase „Pflichtenheft-Erstellung".

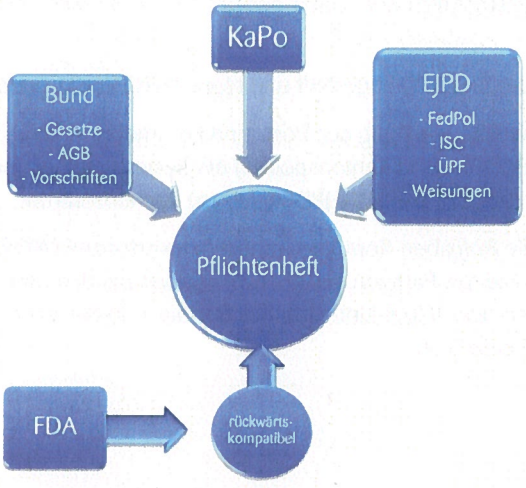

Abbildung 4: Quellen des Pflichtenhefts

Es gibt Anforderungen, die nicht detailliert genug spezifiziert worden sind (Beispiel: was ist genau mit 99.8 % Verfügbarkeit gemeint?), und solche, die nicht widerspruchsfrei umsetzbar sind. Weiterhin gibt es Anforderungen, deren Tragweite sich erst im Projektverlauf gezeigt hat. Ein klarer Verantwortlicher fürs Pflichtenheft und damit für das Scope-Management mit Entscheidungskompetenz ist nicht erkennbar. Scope-Management allgemein scheint dem

Projektleiter zu obliegen: da er nicht über die Entscheidungskompetenz verfügt, kann er zu klärende Themen allerdings lediglich bei den entsprechenden Gruppen vorlegen.

Für das Audit ist in Bezug auf das Pflichtenheft festzuhalten: es gibt kein nachvollziehbares Scope Tracking. Beispiel: es fanden nach Auftragserteilung Workshops mit dem Lieferanten und dem Hersteller statt, aber die Ergebnisse sind nur rudimentär festgehalten und tragen eher den Charakter von Notizen. Somit sind die Auditoren gezwungen, nur mit der Anfangsdokumentation, d.h. mit dem Pflichtenheft (erweitert um einige schwer einschätzbare Kommentare), zu arbeiten. Auf die Frage nach den Abnahmekriterien wird wiederum auf das gesamte Pflichtenheft verwiesen.

Auf Basis des Pflichtenhefts wurde ein Werkvertrag mit einem Lieferanten eingegangen.

Abbildung 5: Aufgaben Besteller (Auftraggeber)– Lieferant – Hersteller

Der Lieferant hat sich mit dem Vertrag verpflichtet, die Software samt Dokumentation für den Aufbau einer Gesamtlösung ISS zu liefern. Der Hersteller war lange Zeit nicht oder nur indirekt in das Projekt involviert, wird aktuell aber mehr und mehr direkt einbezogen.

3.3 System-Abgrenzung

Der Begriff „System" wird im Umfeld des Projekts ISS unterschiedlich verwendet (siehe Abbildung 6).

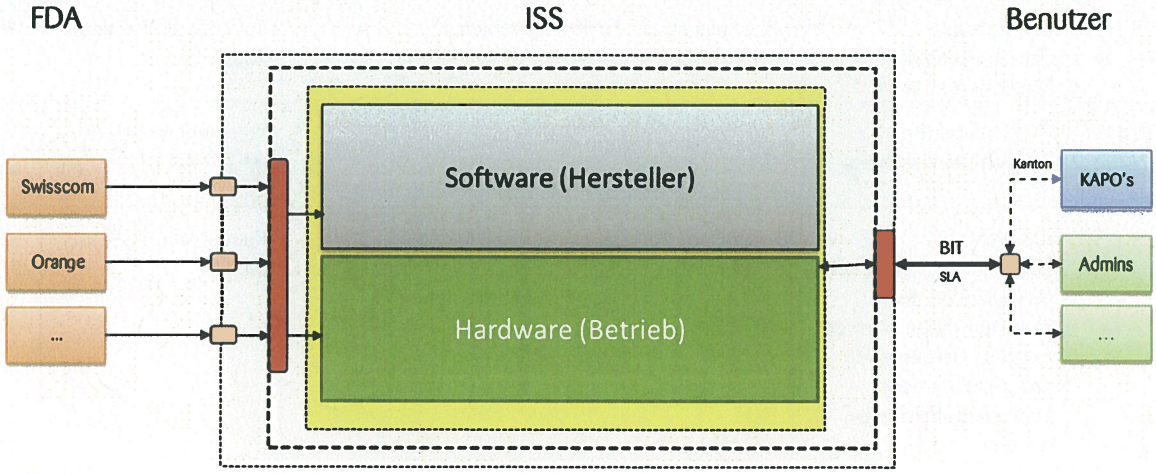

Abbildung 6: Veranschaulichung möglicher Systemgrenzen des ISS

Die gestrichelten Linien sollen mögliche Interpretationen der Systemgrenzen ISS andeuten. Die Pfeile zu und von Hard- und Software sowie die Einteilung Software (im Sinne von „in der Verantwortung des Herstellers") und Hardware (im Sinne von „in der Verantwortung des Betriebs ISC-EJPD") sind nur schematisch angedeutet und nicht so eindeutig, wie es scheinen mag. Zum Gesamtsystem ISS im Sinne einer Beteiligung an der FMÜ zählt der Weg von den FDA übers ISS bis zum Bildschirm der StrafB. Es ist uns nicht bekannt, ob es eine eindeutige Verantwortlichkeit über die gesamte Strecke gibt. Beispiele offener Fragen:

- Wem obliegt die Verhandlung über die Rechtsgrundlagen mit den FDA, wem über die Service Level Agreement (SLA) mit dem BIT?
- Sind diese Rechtsgrundlagen- bzw. SLA-Klärungen im Scope des Projekts oder ausserhalb?
- Wie werden diese Bereiche der „Zulieferung" und „Ausleitung" bei End2End-Tests oder bei Anforderungen (bspw. Reaktion am Bildschirm < 2 sec.) berücksichtigt?

Auch haben die Auditoren kein einheitliches Verständnis über die Systemgrenzen ISS im Rahmen des Projekts identifizieren können. Das Pflichtenheft kann die genauen Abgrenzungen nicht aufzeigen. Damit ist eine Quelle für Unklarheiten im Scope und bei den Themenverantwortlichkeiten im Projekt identifiziert. Auf die Wahrnehmung der System-Abgrenzung wird in den Abschnitten im Anhang eingegangen.

3.4 Rechtsgrundlagen

3.4.1 Aktuelle Anforderungen an das Projekt ISS

Im BÜPF und VÜPF sind diverse Überwachungstypen definiert. Für das Projekt ISS sind nicht alle relevant.

Aktuell stehen drei Systeme zur Verfügung, um die Aufgaben der Fernmeldeüberwachung wahrnehmen zu können:

- System A: Überwachung von CS-Daten
- System B: Überwachung von PS-Daten
- System C: Auskunft von Basisinformationen zu Teilnehmeranschlüssen

Im Scope des Projekts ISS ist nur die Ablöse der Systeme A und B. Diese beiden Systeme bzw. das neue System ISS müssen folgende Überwachungstypen gewährleisten können (gemäss GebV ÜPF, SR 780.115.1):

GebV ÜPF	Überwachungstyp CS	Details	Adressierungs-element	VÜPF Art.
CS 1-3	**[Ü1] Echtzeit-Überwachung der Nutzinformationen**	Übertragung des Fernmeldeverkehrs	Rufnummer, IMEI oder IMSI	16 Bst. a
CS 1-3	**[Ü2] bei Mobiltelefonie: Echtzeit-Überwachung**	Bestimmung und simultane oder periodische Übertragung der Cell ID, des Standorts, der Hauptstrahlrichtung der verbundenen Antenne	Rufnummer, IMEI oder IMSI	16 Bst. b
CS 1-3	**[Ü3] Echtzeit-Überwachung: auch bei Nicht-Aufbau der Kommunikation müssen Angaben bereitgestellt und simultan oder periodisch übertragen werden**	verfügbare Adressierungselemente wie Rufnummern, tatsächliche bekannte Zielrufnummer und ggf. zwischengeschalteter Rufnummern, Mobiltelefondaten (erzeugte Signale, Cell-ID, Standort usw.); Datum und Uhrzeit	Rufnummer, IMEI oder IMSI	16 Bst. c 1-5

N 2	**[Ü4] Suche vermisster Personen: Echtzeit-Verkehrsdaten inkl. Standort**	Technisch wie [Ü2 und Ü3]	Rufnummer, IMEI oder IMSI	16a
	Überwachungstyp Internet	**Details**	**Info zu Zugang und Internetanwendung**	**VÜPF**
PS 1	**[Ü5] Überwachung eines Internetzugangs (Echtzeit)**	Übermittlung sämtlicher Daten	Nutzinformationen und Verkehrsdaten	24a Bst. a
PS 2	**[Ü6] Bereitstellung und simultane oder periodische Übermittlung von Angaben über den Internetzugang (Echtzeit)**	Datum + Uhrzeit, Art der Verbindung / des Anschlusses, Anmeldedaten, verfügbare Adressierungselemente, Parameter der Endgeräte und Teilnehmeridentifikation, ggf. Mobilfunkparameter u.a.	Nutzinformationen und Verkehrsdaten	24a Bst. b
PS 3	**[Ü7] Übertragung der Nutzinformationen der überwachten Anwendung (Echtzeit)**	Abhängig von der Anwendung (siehe auch PR-Anforderungen in [2])	Nutzinformationen	24a Bst. c
PS 4	**[Ü8] Bereitstellung und simultane oder periodische Übermittlung von Kommunikations-parametern aus der Überwachung einer Anwendung (Echtzeit)**	Datum + Uhrzeit, verfügbare Adressierungselemente, Anmeldungsdaten, bei Email die Umschlaginformationen, verfügbare Kommunikationsparameter u.a.	Verkehrsdaten	24a Bst. d

Überwachungstypen wie z.B. Auskünfte, die nicht im Scope des ISS sind, werden in der Tabelle nicht aufgeführt. Auch alle rückwirkenden Überwachungen gehören dazu, denn:

- **Rückwirkend**: Die bei den FDAs gespeicherten Daten werden aktuell per Datenträger direkt an die StrafB übermittelt. Aus technischer Sicht des ISS sind solche Anforderungen (bis auf die Auftragsabwicklung im WMS) nicht im Scope.
- **Echtzeit**: Daten werden direkt von den FDA ans ISS ausgeleitet.
  Die Auswertung der Daten durch die StrafB kann LIVE oder nachträglich erfolgen.

Darüber hinaus obliegt dem ÜPF eine aktive Mitwirkung bei der Triage (d.h. bei der Überwachung von Personen, die einem Berufsgeheimnis wie bei Anwälten unterliegen), um einer möglichen Verletzung des Berufsgeheimnisses vorzubeugen. Es ist nicht erkennbar, dass sich hieraus Anforderungen ans ISS ergeben. Ebenso ausgenommen sind die Anforderungen ans Auftragsmanagement, da hier kein Klärungsbedarf vorliegt.

3.4.2 Mögliche neue Anforderungen an das System ISS durch die Revision des BÜPF

Das BÜPF und im Nachgang auch das VÜPF stehen zur Revision an. Anhand der aktuellen Versionen gibt es 2 Themen, die für das System ISS von Bedeutung werden könnten:

- Langzeitdatenspeicherung: zentrale Speicherung der aufgezeichneten Daten beim Dienst ÜPF mit Abrufmöglichkeiten für die Berechtigten; Datenhaltung bis zu 30 Jahre
- Import und Export: Neu würde auch eine direkte Anbindung weiterer Systeme, z.B. Janus, erlaubt werden.

Im Rahmen des Projekts ISS sind lediglich Konzepte des Herstellers zu sichten, aber keine Implementation von Features, da hierfür die nötige Rechtsgrundlage (noch) fehlt. Beim Sichten der Konzepte ist eine Beurteilung nicht möglich, da die konkreten Anforderungen des ISS noch nicht bekannt sind.

4. Erkenntnisse und Empfehlungen

Im Rahmen des System-Audits wurden durch die strukturierte Befragung anhand der Themengebiete detaillierte Einblicke und Erkenntnisse gewonnen. Die Erkenntnisse beruhen auf den im Anhang aufgeführten Ausführungen des Herstellers und des Betriebes. Die Einführung eines zentralen Fernmeldeüberwachungssystems (ISS) ist wegweisend und unterliegt einer hohen Komplexität in diversen Dimensionen.

4.1 Erkenntnisse

In diesem Abschnitt sind die wichtigsten Erkenntnisse inklusive einer Bewertung aufgeführt. Abbildung 7 zeigt die Bewertung der einzelnen Themengebiete.

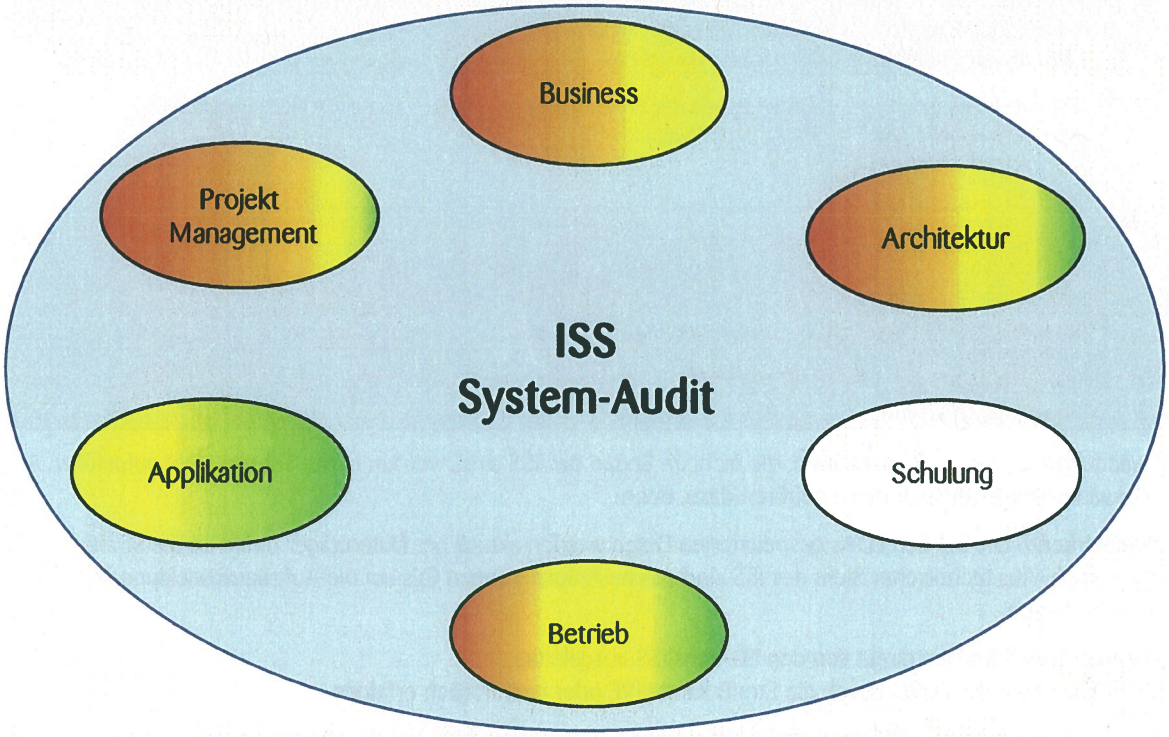

Abbildung 7: Gesamtbewertung ISS (System, Betrieb, Rechtsgrundlagen)

Für die Einzelpunkte wird folgendes Bewertungsschema wird zugrunde gelegt:

Dieser Punkt ist **rein informativ.**
Dieser Punkt ist **sehr kritisch** und **muss umgehend verbessert werden.**
Dieser Punkt ist **wichtig** und **sollte zeitnah verbessert werden.**
Dieser Punkt ist **in Ordnung.** Es besteht **kein Handlungsbedarf.**

4.1.1 Projektmanagement

Das ISS ist aufgrund seines Einsatzgebietes ein Projekt hoher Komplexität. Es zeichnet sich durch eine sehr hohe Anzahl von Stakeholdern aus. Neben geforderten gesetzlichen Rahmenbedingungen, den Datenlieferanten (FDAs), den kantonalen Anforderungen und Interessen, sowie den betrieblichen Rahmenbedingungen und unterliegenden Weisungen, kommt den Anforderungen der Endanwender (StrafB, ÜPF) grosses Gewicht zu.

Die Parteien „**Lieferant**" und „**Auftraggeber**" waren nicht im Scope dieses Audits und wurden daher nicht analysiert.

Die **Anzahl der Stakeholder** und der notwendigen Entscheidungskompetenzen ist kritisch zu beurteilen. Die Entscheidungswege sind für die Auditoren nicht nachvollziehbar.

Das **ISS-Projektteam** auf Seiten ÜPF und ISC-EJPD macht auf die Auditoren trotz der widrigen Projektumstände einen engagierten Eindruck.

Es wurde ein **Hersteller** ausgewählt, welcher einen Standard für die Fernmeldeüberwachung anbietet und pflegt. Gemäss Angaben des Herstellers ist das System bei mehr als 50 Kunden weltweit im Einsatz. Der Hersteller hat dargelegt, dass er eine grosse Expertise im Bereich der Fernmeldeüberwachung vorweisen kann. Der Hersteller ist sehr motiviert, das Projekt zu einem erfolgreichen Abschluss zu bringen und hat mehrfach betont, alle kritischen Fehler zu beheben. Auf Seiten des Herstellers gab es einen Wechsel des Projektleiters. Der Hersteller hat einen eigenen Prozess für das Management seiner Projekte definiert und setzt diesen auch ein.

Die **StrafB** haben die Hoffnung auf einen erfolgreichen Projektabschluss aufgegeben und zeigen momentan geringe Bereitschaft zu einer konstruktiven Mitarbeit, z.B. bei der Testunterstützung.

Der Mehrwert des Lieferanten ist zu hinterfragen, da er primär als Durchlauf agiert und zudem die direkte **Kommunikation** zwischen dem Projektteam und dem Hersteller beeinträchtigt. Die Zusammenarbeit auf technischer Ebene zwischen dem Projektteam und dem Hersteller wurde beidseitig gelobt. Es ist sicherzustellen, dass diese direkte Kommunikation nicht behindert wird.

Von zentraler Bedeutung ist das **Verständnis der Systemgrenze des ISS**. Alle Projektbeteiligte und Stakeholder haben ein unterschiedliches Verständnis hierzu. Im Rahmen des System-Audits wurden pro Partei die Systemgrenzen eruiert und dargestellt. Aufgrund der Unschärfe der Grenzen des ISS-Systems sind auch die Projektverantwortlichkeiten ungenügend ausweisbar.

Auf Seiten des Projektteam ist die **fehlende Entscheidungskompetenz** auffallend. Es gibt bis heute keine zentrale Instanz, welche die Anforderungen an das ISS System entgegennimmt, validiert und zeitnahe Entscheidungen herbeiführt. Dies fördert zunehmend die mangelnde Transparenz der Entscheidungen und die sich hieraus ergebenen Defizite in der Kommunikation mit den ISS-Beteiligten. Dieser Entscheidungsmangel betrifft sowohl das Scope Management als auch die betriebliche Seite.

Kommunikation im Projekt: Die Transparenz ist des Weiteren stark beeinträchtigt, da a) die erkannten Fehler zwischen dem Projektteam und dem Hersteller nicht synchronisiert sind, b) die direkte Kommunikation zwischen dem Projektteam und dem Hersteller stark beeinträchtigt ist und c) der Fortschritt des Projektes schwer ermittelt werden kann (Test-Status, Testplan etc.).

Der Hersteller ist in diesem Projekt **kein Generalunternehmer** und ist nur für die Lieferung der Software-Module und deren Dokumentation verantwortlich. Er installiert somit in diesem Projekt keine schlüsselfertige Lösung beim Kunden. Weder der Hersteller, noch der Betrieb haben Erfahrungen mit einem derartigen Ansatz. Dies führte zu grossen Reibungsverlusten beim Aufbau des Rechenzentrums und der Installation des Systems. Diese sind inzwischen weitgehend behoben.

Test-Management: Dieses komplexe Projekt wurde bis Ende 2012 nicht durch ein dediziertes und erfahrenes Test-Management begleitet. Seit Januar 2013 wurde ein externer Testmanager eingestellt. Seither ist eine deutliche Verbesserung in diesem Bereich zu erkennen. Es muss sich allerdings erst noch zeigen, ob diese Massnahme ausreichend ist. Weiterhin ist die Weiterführung dieser Aufgabe nach dem Weggang des externen Testmanagers noch unklar, da der Nachfolger aktuell nicht über ausreichende Kenntnisse in diesem Bereich verfügt.

Test-Planung: Aktuell werden lediglich Komponententests durchgeführt. Es ist dringend notwendig, auch weitergehende Tests wie UAT, Performance und Failover zu planen und durchzuführen.

4.1.2 Business

Von zentraler Bedeutung ist die Analyse der funktionalen Anforderungen (Business) und der nicht-funktionalen Anforderungen (Qualitäten und Einschränkungen des Systems).

Aufgrund der sich ändernden gesetzlichen Vorgaben und des technischen Fortschrittes wird das System ISS einem stetigen Wandel unterworfen sein.

Die sog. AR- und K-Anforderungen der Funktionsliste [2] weisen eine gute Rechtskonformität auf. Bei einzelnen Punkten gibt es Klärungsbedarf, bei anderen Punkten wird im Zusammenhang mit der Umsetzung des Benutzerkonzepts (z.B. Themen zu mehreren Targets) auf den Datenschutz zu achten sein, doch dieses Konzept und seine Umsetzung waren nicht Gegenstand der Prüfung.

Die funktionalen Anforderungen sind auf einer sehr hohen abstrakten Ebene beschrieben, welche einen erheblichen Interpretationsspielraum zulassen.

Auf Basis der Funktionsliste sind die funktionalen Anforderungen durch das Standard-Produkt des Herstellers weitgehend unterstützt. Es besteht in einigen Bereichen noch Detailierungsbedarf bei den Anforderungen, um ein gemeinsames Verständnis aller Stakeholder zu erreichen.

PS-Anforderungen aus Endanwender-Sicht sind im Pflichtenheft [1, 2] bis auf eine Anwendungsliste weniger konkret als im CS-Bereich.

Spezifische Anforderungen der StrafB sind ungenügend spezifiziert und daher nicht Bestandteil des Audits. Die Benutzerszenarien weisen eine sehr grobe Granularität auf. Messbare Vorgaben sind hierbei die Ausnahme.

Die nicht-funktionalen Anforderungen (NFR) unterliegen diversen Weisungen (gesetzlichen, betrieblichen, kantonalen etc.) und Vorgaben des Pflichtenhefts. In einem komplexen System wie dem ISS ist es notwendig, die NFR sorgfältig betreffend der geforderten Qualitäten und der gegebenen Einschränkungen abzuwägen. Sowohl auf Seiten des Projektteams als auch des Herstellers gibt es keine konsolidierte Beschreibung der NFR. Da diese massgeblich das Design der Lösung beeinflussen, ist hier ein erhebliches Risiko identifiziert worden.

Die **Verfügbarkeitsanforderung von 99.8%** wurde im Pflichtenheft beschrieben. Alle befragten Beteiligten (Projektteam, Betrieb, Hersteller und StrafB) haben eine differenzierte Meinung bzgl. der Verfügbarkeit.

Spezifische Anforderungen vom Auftraggeber können durch den Hersteller umgesetzt werden und dabei in den Standard einfliessen. Notwendig sind hierfür ein gegenseitiges Verständnis der Anforderungen und eine Abnahme der Hersteller-Spezifikation durch den Auftraggeber.

4.1.3 Architektur

Im Rahmen des Audits sind diverse Fragen über den Reifegrad des Produktes des Herstellers gestellt worden. Diese umfassen u.a. die Eignung des Produktes für die Schweiz als auch der Erweiterbarkeit und Integrationsfähigkeit.

Der Hersteller hat ein Standard FMÜ-System entwickelt, welches beim ISS zum Einsatz kommt. Es wurden spezifische Erweiterungen (z.B. WMS und Anpassungen an die FDAs) durchgeführt.
Aufgrund der stetigen Weiterentwicklung ihres Standardproduktes enthält es momentan noch **signifikante Teile des Vorgängersystems**. Laut Aussage des Herstellers werden in den kommenden Produkt-Releases diese Komponenten vollständig in die neue Architektur überführt. Dies führt zu einer Reduktion der Komplexität (Anzahl Server, Konfigurationen etc.) und einer konsequenten Standardisierung. Dies bedingt auch, dass die Software Komponenten des ISS aktualisiert werden.
Die Architektur zeigt **konzeptionell einen guten Reifegrad auf**. Die Trennung der Verarbeitung in Stufen ist nachvollziehbar und stellt sicher, dass die Datensicherheit von der Erfassung bis zur Persistierung in der Datenbank gewährleitstet wird.
Die Architektur ist ausgelegt auf die Verarbeitung von CS- und PS-Daten, welche in grösseren Datenblöcken verarbeitet werden.
Die Architektur weist **zwei getrennte Datenflüsse für CS und PS** auf. Die detaillierte Beschreibung der Datenflüsse konnte durch direkte Befragung der Entwickler geklärt werden. Eine End-2-End-Beschreibung der Datenflüsse ist seitens des Herstellers ungenügend.
Die **LIVE-Beobachtung** ist eine zentrale Komponente. Die Daten werden auf einem separaten Pfad durch das System geleitet. Die Dekodierung erfolgt im Investigator. Damit können diese schneller durch das System geleitet werden, allerdings werden die Performanceanforderungen für den Investigator grösser (Belastung des Citrix-Servers).
Im Bereich der Konnektivität der StrafB auf das LIVE-Gespräch gibt es noch einige Bugs, die gemäss Hersteller behoben werden.
Die Architektur basiert im Kern auf einem **dateibasierten Transfer der Daten** zwischen den einzelnen Verarbeitungsstufen.
Die Hersteller-**Dokumentation der Systemarchitektur** ist **unzureichend**. Zum einen gibt es unterschiedliche Namenskonventionen der gesichteten Dokumentationen, da Sie zum Teil aus dem Schwerpunkt Verkauf stammen (Sales-Material). Des Weiteren ist die Dokumentation sehr stark betrieblich und hardwarenah beschrieben. Eine High-Level Architektur der funktionalen Blöcke ist im Audit unzureichend präsentiert worden.
Auf Seiten des Projektes ist die **Dokumentation der Gesamtarchitektur** ebenfalls **unzureichend**. Dies erschwert insbesondere die Analyse von Änderungen am ISS-System.
Schwerwiegend ist der Umstand, dass wichtige und **zentrale Architekturentscheide ungenügend dokumentiert** worden sind und diese nicht zentral erfasst wurden. Dies trifft sowohl auf den Hersteller, als auch das Projekt selbst zu. Hierdurch sind die Nachvollziehbarkeit und die Kommunikation von Entscheidungen ungenügend gegeben. Daraus folgt der von den Auditoren bei allen Interviews gesehene grosse Interpretationsspielraum aller Beteiligten.
Die zentrale Komponente der Architektur bildet die Datenbank. Diese muss sowohl die Last der Datenannahme, den Zugriff der Benutzer und die externen Komponenten (Archivierung etc.) unterstützen. Die **Skalierung der Datenbank** und die Sicherstellung der Performanz sind **herausfordernd**. Der Hersteller ein eine sehr grosse Expertise im Bereich der Datenbanken. Alle Schnittstellen werden mittels Stored Procedures realisiert, um die sicherheitsrelevanten Aspekte auf der Datenbank sicherstellen zu können. Externe Integration und Erweiterungen können somit nur über die Stored Procedures erfolgen. Die Datenbanken sind jeweils mit dem Vorgängerrelease kompatibel, dies erlaubt einen schrittweisen Ausbau des Systems.

Es gilt seitens des Betriebes sicherzustellen, dass die IO-Performanz der Datenbank zum NetApp-Storage auch für zukünftige Ausbaustufen des Systems ausreichend ist.

Momentan ist die **Verfügbarkeit** nicht garantiert, da die rechtlichen Verordnungen mit den FDAs nicht ausreichend sind.

Seitens der Auditoren wurde mehrfach hinterfragt, was die hohe Verfügbarkeit bedeuten soll. Zwecks Sicherstellung der Datenannahme ist die sogenannte Ausleitung zu 100% verfügbar auszulegen, da sonst Daten verloren gehen können (s. 4.1.3.2). Die nachfolgende Verarbeitungskette kann nach einem Unterbruch wieder aufgenommen werden, ohne Daten zu verlieren. Businessrelevant ist, dass die StrafB die erhobenen Daten sichten, analysieren und bewerten können. Das LIVE-Feature kann nicht zu 99.8% gesichert werden, da die FDAs keine parallele Zuleitung der laufenden Gespräche durchführen (CS).

Durch die hohen Anforderungen hinsichtlich Verfügbarkeit des Gesamtsystems und die Redundanz über zwei Standorte wurde die Komplexität des Designs deutlich erhöht.

Datenverlust im Disaster-Fall: Das ISS-System ist nicht in der Lage im Disaster-Fall sicherzustellen, dass keine Daten bei der Annahme (Eintrittspunkt ISS) verloren gehen. Insbesondere ist die Anlieferung der HI2-Daten nicht redundant ausgelegt und die CS-Übernahme bei einem Ausfall der physischen Einheit nicht garantiert.

Ausfälle der folgenden Komponenten können zu Datenverlusten führen:

- Aktive Gespräche können nicht zum anderen Standort transferiert werden, daher gehen diese vollständig verloren.
- Die empfangenen Daten werden erst in einer späteren Verarbeitungsstufe zwischengespeichert. Sollten vorangeschaltete Komponenten ausfallen, könnten Daten verloren gehen. Ab diesem Punkt wird sichergestellt, dass empfangene Daten nicht mehr verlorengehen können.
- Beim Ausfall einer Komponente könnte es vorkommen, dass Puffer (konfigurierbar) in vorherigen Systemen überlaufen, bevor der Failover auf Ersatzkomponenten durchgeführt wurde.
- Eventuelle Time-Outs (z.B. Gesprächslänge) können zu Datenverlust führen, wenn das Maximum eines Time-Outs erreicht wird.

Die FDAs puffern keine Daten, so dass Datenverlust droht, wenn die Gegenstelle im ISS die Daten nicht mit dem gleichen Speed empfängt. Es empfiehlt sich eine Appliance einzuführen, welche die vollständige Entgegennahme der Eingangsdaten (Ausleitung) sicherstellt und auch im Disaster-Fall redundant ausgelegt ist.

Es kann nicht ausgeschlossen werden, dass bereits auf Seiten der FDAs Pakete verloren gehen.

Latenz von <2 Sekunden bei der LIVE-Beobachtung: Der Hersteller ist momentan nicht in der Lage, die Latenz im LIVE-Stream innerhalb seines Systems zu messen, und behauptet, dass es weniger als 2 Sekunden sind. Die subjektive Beobachtung der Auditoren am Demonstrationssystem des Herstellers erweckt den Eindruck, dass schon dort die Verzögerung mehr als 2 Sekunden beträgt. Messungen des Projektteams bestätigen diese Vermutung. Hier ist von einer Verzögerung von 6-12 Sekunden die Rede.

Es wird dringend empfohlen hier eine entsprechende Instrumentierung vorzunehmen und Messungen durchzuführen.

Sofern im Investigator mehrere Targets gleichzeitig beobachtet werden, kann es passieren, dass die Decoder des Investigators überlastet sind und deshalb eine Verzögerung beobachtet werden kann.

Datenbank kann zu einem Engpass werden

Die Anwendung ISS ist Datenbank-zentrisch gebaut, das heisst alle Daten werden

- in die DB geschrieben
- indexiert
- durch Post-Processing Anwendungen aktualisiert (z.B. HI2 Zusammenführung, Archivierung etc.)
- und von den Benutzern zugegriffen.

Die Datenbanken werden durch die direkte Anbindung der Fat-Clients (2-Tier-Architektur), als auch durch das Postprocessing und Archivierung belastet. Hierdurch kann nicht garantiert werden, dass genügend Leistung für die Speicherung der Input-Daten bereitsteht.

Der Durchsatz der Datenbank in den Bereichen Rechenleistung (CPU) und Speicher (I/O) muss entsprechend gewährleistet sein und für künftiges Wachstum skalieren.

Die Skalierung der Datenbanken erfolgt durch Nutzung von Data Nodes, welche bei einem weiteren Wachstum zusätzliche dedizierte NetApp-Storage benötigen.

4.1.4 Applikation

Der Hersteller verfügt über sehr viel Expertise, sowohl fachlich als auch technisch. Durch die stetigen technischen Neuerungen (Protokolle, Bandbreiten etc.) ist der Hersteller in der Lage die Auswirkungen auf Ihr Standard-Produkt zu analysieren und ggfs. die Architektur anzupassen.

Der Fat-Client enthält sehr viel Funktionalität, was zu einem komplexen Bedienkonzept führt. Der Investigator ist ein sehr mächtiges Werkzeug mit einer erhöhten Komplexität bei der Bedienung. Es besteht die Möglichkeit, das Erscheinungsbild und die Funktionen anzupassen. Mit dieser Applikation stehen den StrafB deutliche mehr Funktionen als im bestehenden System zur Verfügung.

Die Clients pollen die Information direkt von der Datenbank und können sich gegenseitig eingeschränkt über das Konfigurationstools notifizieren. Dies führt dazu, dass einzelne Clients teilweise unterschiedliche Informationen anzeigen.

Die Testautomatisierung im Bereich UI und DB sind noch nicht in ausreichendem Masse vorhanden, werden vom Hersteller aber immer mehr ausgebaut.

Gelieferte Releases sind per Definition vom Hersteller nicht vollumfänglich getestet worden.

GA-Releases durchlaufen einen detaillierten Test.

Der Hersteller verfügt über einen definierten Entwicklungsprozess und lebt diesen auch.

4.1.5 Betrieb

Der Aufbau der Infrastruktur basiert auf dem aktuellen Stand der Technik. Die Software-Komponenten können zentral überwacht werden und die Failover Mechanismen im Bereich VMWare und Citrix sind solide.

Im Speicherbereich wurde konsequent auf Grundlage einer GL-Entscheidung auf IP-Protokolle gesetzt (iSCSI, NFS etc.). Für den Datenbank-Bereich mag dies zurzeit kein Engpass darstellen, allerdings ist bei datenbank-intensiven Anwendungen eine Fibre-Channel-Lösung zu bevorzugen. Sollte sich das IO-Verhalten der Datenbank signifikant verschlechtern, so ist der Wechsel auf Fibre-Channel zu tätigen. Dies kann durch sorgfältiges Monitoring seitens des Betriebs sichergestellt werden.

Der Betrieb hat intensiv mit den Beteiligten die meisten Probleme beim **Aufbau der Hardware** unter direkter Mitwirkung des Herstellers gelöst.
Netzwerkseitig ist die Zuständigkeit bis zum BIT Netzwerk geregelt. Eine Verantwortung bis zum Arbeitsplatz des Endanwenders kann nicht wahrgenommen werden, da die Netzwerke nicht im Hoheitsgebiet des Betriebes liegen.
Der Betrieb des ISC-EJPD ist der Auffassung mit CS in die Pilotierung gehen zu können. Es muss sich noch zeigen, dass das ISC-EJPD in der Lage ist, dieses System zu betreiben. Daher ist eine enge Kooperation mit dem Hersteller zu favorisieren, welche bisher auch sehr gut funktioniert hat.
Nach eigenen Angaben, hat der Betrieb bisher noch nie das System ohne Unterstützung durch den Hersteller deployed. Entsprechende Versuche sollten umgehend in der Pilotierungsphase erfolgen, um sicherzustellen, dass das hierfür benötigte Know-How auch verfügbar ist.
Erschwerend erweist sich, dass teilweise **physikalische Ressourcen** wie Netzwerk, Storage noch mit anderen Applikationen **geteilt** werden. So nutzt auch das PoliceCorp das physische Netzwerk, welches logisch getrennt ist. Für die Skalierbarkeit des Systems ist langfristig die Verwendung von dedizierten physikalischen Ressourcen zu bevorzugen.
Die **Weisungen für das Rechenzentrum** sind zu streng und für ein FMÜ-System nicht angemessen. Dies führt zu Einschränkungen in Bezug auf Anforderungen oder zu übermässig komplexen technischen Lösungen (99.8% Verfügbarkeit). Weisungen und Vorschriften des Bundes und des EJPD sollten in Bezug auf das ISS geprüft und im Zweifelsfall zugunsten des ISS ausgelegt bzw. geregelt werden: die hohe Komplexität ist in den Weisungen nicht berücksichtigt und bedarf spezieller Auslegungen und Anpassungen. Hierfür braucht es eine zentrale und kompetente Entscheidungsinstanz: aktuell werden einige Themen als ‚heisses Eisen' weitergereicht und behindern dadurch sowohl den Betrieb als auch den Einsatz des ISS. Wenn der Bund ein solches System betreiben will, muss er die nötigen Massnahmen dafür ergreifen.

4.1.6 Schulung

Nicht im Scope des System – Audits.

4.2 Empfehlungen

Basierend auf den Interviews, der Nutzung von etablierten Praktiken und den gewonnen Erkenntnissen sind im folgenden Kapitel Empfehlungen erarbeitet worden.

4.2.1 Projektmanagement

Sowohl das Projektteam (ÜPF und ISC) als auch der Hersteller sind der Auffassung, dass das Projekt erfolgreich umgesetzt werden kann. Im Rahmen des System-Audits lassen sich die Empfehlungen aus dem Projekt-Audit bestätigen. Von tragender Bedeutung ist der unabdingbare Wille jeder involvierten Partei, dieses Projekt zum Erfolg zu führen. Hierfür ist das Vertrauen aller in die ISS-Lösung eine zentrale Vorrausetzung. ISS ist ein komplexes Projekt eingebettet in ein Umfeld mit partiellen Interessenslagen. Unabhängig von der Wahl eines Herstellers zur Fernmeldeüberwachung gelten die folgenden Aspekte sicherzustellen:

- Schärfung der Projektkompetenzen (AKV) zwischen ISC-EJPD und ÜPF.
- Stärkung des Projektausschusses zu einem Entscheidungsgremium mit regelmässigen Sitzungsterminen.
- Zeitnahe Kommunikation projektrelevanter Entscheidungen.
- Etablierung einer kollaborativen und engen Zusammenarbeit mit dem Hersteller.

- Schärfung des Projektscopes: Grauzonen identifizieren und in Schwarz oder Weiss (in scope oder out of scope) überführen.
- Verantwortlichen für fachliche und technische Entscheidungen definieren und mit ausreichenden Kompetenzen versehen.
- Alle Parteien testen aktiv das System und sind somit integraler Bestandteil des Test-Teams. Jeder stellt sicher, dass Fehler etc. proaktiv gemeldet werden und der Abgleich zwischen den Tracking-Systemen (Intern/Hersteller) erfolgt.
- Erarbeitung der konkreten Testszenarien und Abnahmekriterien sowie die Einführung von Regressionstests zur Sicherstellung der qualitativen Aspekte.
- Definierte Vorgehensweise für Fehlerhandling durch exakte Angaben zur Reproduzierung (Testbeschreibung, Testdaten, Logfiles) erarbeiten, etablieren und einführen.
- Regelmässige Statusaktualisierung aller Beteiligten (insbesondere StrafB) schafft Transparenz und Vertrauen.
- Sicherstellung der direkten Kommunikation zwischen Projekt-Team, Hersteller, ÜPF, Betrieb. Es erweist sich als vorteilhaft, einen technischen Ansprechpartner des Herstellers vor Ort zu haben.
- Etablierung eines „Single Point of Contact" zwischen Projekt und Hersteller für die Herbeiführung von Entscheidungen.
- Bei Auswahl nach Möglichkeit zugunsten einer Komplexitätsreduktion entscheiden.
- Ernennung eines ISS-Lead-Architekten, welcher die Anforderungen an die Architektur validieren kann, deren Auswirkungen aufzeigen und entscheidungsberechtigt ist.

Für das weitere Vorgehen dieses wichtigen Projektes ist es unabdingbar, konsequent die Fakten mit den Beteiligten zu erörtern und Lösungen zu erarbeiten, welche zur Umsetzung kommen. Politische Diskussionen gehören zum Projekt-Umfeld und in die entsprechenden Gremien, dürfen das Projekt aber nicht lähmen. Diskussionen sollten sachlich und fundiert erfolgen mit klaren Anweisungen an das Projekt, wie bis zur Klärung weiter zu verfahren ist.

Wir empfehlen dringend die Einführung von vertrauensbildenden Massnahmen. Kritiker gilt es einzubinden, wenn die Kritik objektiv und sachlich fundiert ist. Destruktives Verhalten sollte umgehend geahndet werden. Einer der Schlüssel in diesem Kontext ist die umgehende Verbesserung der Kommunikation zwischen allen Beteiligten.

4.2.2 Business

Erfolgreiche Projekte haben ihren Ursprung in einer soliden Erhebung und Erfassung der funktionalen Anforderungen. Bezugnehmend auf die Kriterien des Internationale Requirements-Engineering Boards sind die Anforderungen und Kriterien des ISS-Systems auf einer sehr hohen Abstraktionsebene beschrieben worden. Auf dieser Abstraktionsebene erfüllt der Hersteller die Anforderungen.

Auf Grundlage der Interviews hat sich herausgestellt, dass die StrafB ein anderes Verständnis der Anforderungen haben. Wie bereits im Projekt-Audit ausgeführt, ist die Spezifikation keine Kernkompetenz der StrafB, eine gezielte Unterstützung im Zusammenhang mit dem Scope-Management wird daher empfohlen.

Beispiel verschlüsselte Internetdaten: der Umgang mit ihnen ist ungenügend spezifiziert. Sie können vom System entgegen genommen und gespeichert werden. Ohne gültige Schlüssel sind die Daten (z.B. Skype-Calls oder SSH Secure Shell) im Investigator nicht verwendbar. Dies ist keine Unzulänglichkeit des Herstellers, sondern ein Umstand, welcher durch die Verschlüsselung im IP-Bereich hervorgerufen wird.

Folgende Empfehlungen sollten umgehend angegangen werden:

- Scope-Management des Projekt (siehe Abbildung 8):
    - Klare Definition der Verantwortungen mit der notwendigen Entscheidungskompetenz bei einer Person über die fachlichen Anforderungen (Rolle „Produkt-Manager"). Diese Person geniesst das Vertrauen aller Beteiligten.

- Klare Dokumentation (Nachvollziehbarkeit) der Anforderungs-Spezifikation, deren Abnahme und Gültigkeit sowie deren Änderungen.
- Identifikation von Grauzonen und Sicherstellung, dass diese geklärt werden: Triage in-scope vs. out-of-scope. Klärung der unzureichend spezifizierten Anforderungen.
- Professionelle Unterstützung bei notwendigen Nach-Spezifikationen.
- Klare Abstimmung mit dem Hersteller (Grob-Spez – Fein-Spez – Entscheidung) mit der notwendigen Dokumentation der Entscheidungen.

- Rolle „Informatik-Rat ISS" beim Bund oder beim EJPD einführen, um klare Entscheidungen bei Weisungskonflikten für das ISS zeitnah herbeiführen zu können. Weisungen haben einen massiven Einfluss auf die Komplexität des Systems (z.B. 2 gleiche Systeme an 2 Standorten) und können sogar kompromittierend wirken (z.B. Datenverlust durch AntiVirus).

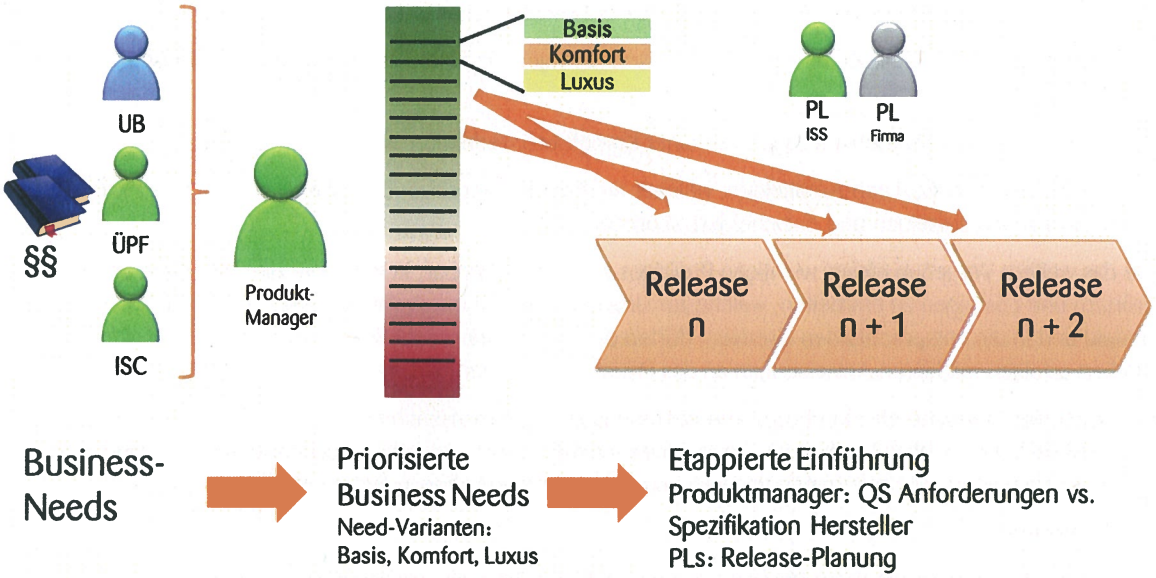

Abbildung 8: Vorschlag zum Scope-Management mit „Produkt-Manager"

4.2.3 Architektur

Die Architektur des ISS ist darauf ausgelegt einen möglichen Datenverlust auszuschliessen, um die Beweiskraft nicht zu gefährden. Daher werden die entgegengenommen Daten in einer Verarbeitungskette in der Datenbank persistent hinterlegt.

Ein gemeinsames Verständnis der nicht-funktionalen Anforderungen (NFR) ist in diesem Projekt ungenügend gegeben. Wir empfehlen daher umgehend diese mit hoher Priorität zu klären, da Sie erheblich die Komplexität der Lösung reduzieren können. Aus Sicht der Beweisführung ist es unabdingbar, dass alle Daten verlustfrei gesichert werden. Durch fehlende Rechtsgrundlage mit den FDAs ist dies bereits bei der Anlieferung nicht gewährleistet. Damit ISS die Daten verlustfrei aufzeichnen kann, müssen einzelne Komponenten die höchste Verfügbarkeit aufweisen (Input). Bei anderen Komponenten muss diese nach Meinung der Auditoren nicht unbedingt so hoch sein. Walkthrough-Szenarien sind ungenügend definiert worden, um die NFRs überprüfen zu können.

Definierte Messpunkte für einen Performanz-Nachweis sind ungenügend definiert worden. Dies gilt es zu bereinigen, um die NFRs überprüfen zu können und ggfs. das System optimieren zu können.

Die grundlegende Architektur des ISS macht einen soliden Eindruck und ist ein Standard, welcher kontinuierlich weiterentwickelt wird. Für spezielle Anforderungen empfehlen wir den dedizierten Einsatz von off-the-shelve-Produkten (z.B. 100% Entgegennahme der Daten) und deren Integration anstelle einer aufwendigeren Software-Lösung.

Folgende Empfehlungen sollten umgehend angegangen werden:

- Klärung und Festlegung der NFRs mit allen Projektbeteiligten (z.B.: Wieviel Verfügbarkeit für welche Teile des Systems?).
- Dokumentation des Systemkontextes und aller relevanten Architekturentscheidungen inklusive der Begründungen.
- Messung der Latenz bei der LIVE-Beobachtung.
- Klärung relevanter offener Punkte
    - Verlustfreie Entgegennahme der Daten für PS
    - Virenscanner

4.2.4 Betrieb

Der Aufbau des betrieblichen Umfelds entspricht dem Stand der Technik und bietet Kapazitäten für weiteres Wachstum. Besonderes Augenmerk liegt hierbei auf dem Bereich der Datenbankanbindung zum Storage. ISS ist eine datenbank-zentrische Anwendung und benötigt gerade dort ein hohes Mass an Durchsatz. Der dortige Einsatz von iSCSI könnte in Zukunft zu einem erheblichen Flaschenhals führen.

Der Aufbau des Wissens über die Datenflüsse des Systems ist zu stärken, um im Fehlerfalle proaktiv handeln zu können. Hierfür ist auch ein dediziertes Verständnis der Software Module erforderlich.

Das Monitoring und System Management entspricht dem Stand der Technik.

Die Grenze des ISS-Systems ist aus betrieblicher Sicht klar geregelt und beginnt beim Eintritt der Daten von den FDAs und endet beim Versand der Daten auf das BIT Netzwerk. Die SLAs gilt es dringend zu definieren.

Folgende Empfehlungen sollten umgehend angegangen werden:

- Diverse Weisungen gilt es für den Betrieb zu vereinfachen und anzupassen.
- Das Sharing des Netzwerkes, des Storage und anderen Komponenten muss für ISS vermieden werden.
- Definition von festen Wartungsfenster, welches eine massive Reduktion der Komplexität im ISS begünstigt. Dieser Mechanismus hat auch bisher sehr gut funktioniert. Laut Aussagen des Betriebs ist in den vergangen 10 Jahren ist nur 3-mal ein Wartungsfenster wegen dringender Überwachungstätigkeiten verschoben worden.
- Überdenken der Patch-Anforderungen und wie hoch ist die Dringlichkeit tatsächlich? Diese Weisung ist bedingt zu befolgen, da das Risiko für einen Ausfall des Systems und somit der Unterbruch der Überwachung wesentlich höher zu bewerten ist.

4.2.5 Zusammenfassung

Das ISS ist ein Standard-Produkt des Herstellers und wurde um entsprechende Komponenten (WMS) erweitert. Der Hersteller hat glaubhaft dargelegt, wie er den Standard pflegt, erweitert und kundenspezifisch ergänzen kann. Er verfügt über das notwendige fachliche Wissen im Bereich FMÜ und hat eine sehr solide Basis an guten Software-Ingenieuren. Das System ist im Wandel begriffen und die Architektur bildet eine gute Basis. Für eine LIVE-Beobachtung aller Targets (ausser Audio) ist es aus heutiger Sicht nur bedingt einsetzbar. Das ISS stellt sicher, dass alle Daten persistiert werden. Es kann verschlüsselte Daten speichern aber nicht verarbeiten.

Unsere Empfehlung lautet:

- Einführung des ISS in der Pilotphase für CS. Behebung der Fehler und Optimierung des Systems in weiteren Ausbaustufen.

- Sorgfältiges Testen des Gesamtsystems:
  - Sytemtests
  - User Acceptance Tests
  - Failover-Tests
  - Performance-Tests
- Umgehende Klärung des Verfügbarkeitskonzeptes für PS unter Verwendung von spezialisierten Produkten.
- Überprüfung der nicht-funktionalen Anforderungen.

Das System wird einer permanenten Weiterentwicklung unterworfen sein: Mehr Überwachungsfunktionalität, grössere Datenmengen und weitere Analysefunktionalitäten. Alle Elemente der Gesamtkette bis hin zu den Clients müssen hierfür permanent ausgelegt und skaliert werden. Der Hersteller hat eine Roadmap vorgestellt, wie diese Entwicklung von statten gehen könnte. Mittelfristig gibt es die Verbesserungsmassnahme der DB-Durchsatz Optimierung anhand der Umstellung von iSCSI auf Fibre Channel.

Die Auditoren sind der Meinung, dass die noch fehlenden Anforderungen aus dem Pflichtenheft noch in das System integriert werden können. Allerdings gibt es hier noch einen grossen Unterschied zu den Anforderungen der Benutzer (StrafB). Deren Akzeptanz des Systems wird zum grössten Teil davon abhängen, inwiefern die kritischen Punkte noch umgesetzt werden.

Das System sichert die Entgegennahme und die Speicherung der Daten sowie deren Analyse. Somit ist eine Fernmeldeüberwachung gemäss Gesetz gegeben.

5. Ziele und Fragestellungen

In diesem Abschnitt sind die Ziele und Fragestellungen dieses Systemaudits inklusive einer Bewertung aufgeführt. Hierfür wird folgendes Bewertungsschema wird zugrunde gelegt:

5.1 Ziele des Audits

5.1.1 [Z1] Wie soll mit ISS fortgefahren werden: sanieren, portieren oder neu evaluieren?

Im Management-Summary ist die Empfehlung der Auditoren ausführlich beschrieben.

5.1.2 [Z2] Hat der Lieferant das geliefert, was er angeboten hat?

Im Abschnitt 4.1.2 wird auf die Anforderungen des Pflichtenhefts Bezug genommen: das abstrakte Niveau der Anforderungen ermöglichte dem Hersteller eine Zusage im Standard oder Releaseplan. Die vorhandene Dokumentation lässt eine weiterreichende Beurteilung nicht oder nur punktuell mit viel Aufwand zu.

LIVE-Beobachtung: Die Ergebnisse des System-Audits beim Hersteller können den geäusserten Verdacht, die LIVE-Funktionalität sei nachträglich (und insbesondere nach Bestellung eingebaut worden) nicht bestätigen. Die Nachbesserungen zeigen hingegen, dass die Bedürfnisse der StrafB unterschätzt wurden.

Im Sep. 2011 sind lediglich 17 AR-Anforderungen als noch nicht geliefert markiert, 3 davon waren als ‚im Standard' gekennzeichnet, die anderen 14 als ‚Release' oder ‚Individualentwicklung'; bei einigen gelieferten Funktionen sind Erweiterungslieferungen angekündigt. Insgesamt gibt es 165 AR-Anforderungen.

Einige Einträge in [2] können als Indizien für eine ungenügende Abstimmung zwischen Lieferant und Hersteller gedeutet werden: AR6.1 - AR6.4 wurden als ‚Im Standard' in der Offerte gekennzeichnet. In der ISS-Funktionsliste mit Kommentaren vom 30.4.2012 vermerkt der Lieferant, dass diese Funktionalität nicht im System integriert ist und der Kunde eine Lösung von Drittprodukten akzeptiert.

5.1.3 [Z3] Kann der Lieferant ein lauffähiges System liefern?

Der Lieferant ist grundsätzlich in der Lage ein lauffähiges System zu liefern.

Aktuell erfüllt das System allerdings noch nicht alle Anforderungen. Es sind daher noch Nachbesserungen notwendig (siehe auch Abschnitt 4.2) oder Neu-Entscheidungen der NFRs zur Reduktion von Komplexität.

Im PS-Bereich gibt es noch offene Punkte hinsichtlich Redundanz und Skalierbarkeit bei steigendem Datenvolumen im IP-Bereich.

Für ein lauffähiges Gesamtsystem müssen weiterhin alle Teile (so auch die HW, der Betrieb, die FDAs und die Netzwerke zu den StrafB) nahtlos ineinandergreifen. Auch hier gibt es noch an einigen Stellen Nachbesserungsbedarf (siehe auch Abschnitt 4.2)

5.1.4 [Z4] Gegenüberstellung von Rechtsgrundlagen und Anforderungen

AR- und K-Anforderungen [2]: Der grobe Gesamt-Überblick aus Sicht BÜPF / VÜPF ist positiv.

- Einzelne Themen sind in den geprüften Rechtsgrundlagen nicht enthalten und vermutlich an anderer Stelle (kantonal, StPO, DSG) geregelt (siehe „Anforderungen an StrafB" weiter unten).
- Einzelne Themen wären zu überprüfen, ob hier Anpassungsbedarf bei den Rechtsgrundlagen besteht oder ob sie implizit abgedeckt sind. Hierfür bedarf es eines tieferen juristischen Verständnisses, als es bei den Auditoren vorliegt. Ausführungen hierzu folgen weiter unten.
- Einzelne Themen sind in [2] zu grob beschrieben. Hier kommt es auf die aktuelle Umsetzung an, um z.B. die Einhaltung der nötigen Datenschutz- und Sicherheitsanforderungen zu prüfen. Damit ist vor allem das Benutzerkonzept mit Berechtigungen und Verwaltung im Fokus, das im Rahmen des Audits nicht überprüft wurde.

Es wurde nicht geprüft, ob Anforderungen zusätzliche Anpassungen in der GebV ÜPF (SR 780.115.1) rechtfertigen könnten.

Pflichtenheft und Weisungen für den Betrieb: Diverse Weisungen beinhalten Komplexitätstreiber oder unnötige Risiken (AntiViren-Programm führt im Zweifelsfall zu Datenverlust). Die diversen Anforderungsquellen (Datenschutz, Bund, Behörde, ISC-EJPD, Projekt) stehen teilweise im Widerspruch. Hier bedarf es einer Triage und dem Ausnutzen von Auslegungsspielräumen zugunsten des ISS. Themen sind Wartungsfenster, Sicherheits-Patches, Verfügbarkeit, Datensicherheit (kein Datenverlust), AntiViren-Programm-Einsatz.

Anforderungen an StrafB: In den geprüften Rechtsgrundlagen wird nur von der „zuständigen Behörde" gesprochen, ohne auf spezifische Anforderungen an sie einzugehen. Themen wie Whitelist für Alarmierungen (AR4.3), Systeminformation (AR7.4) oder Target-Statusinformationen (AR7.5), die in den Themenkomplex der Benutzerrechte und –verwaltung gehören, können daher vorliegend nicht beurteilt werden.

Löschen von Verschriftungen (AR5.4): Die Anforderung ist in Ordnung. Der Kommentar vom Lieferanten ist jedoch verwirrend: es muss in dem Kontext sichergestellt sein, dass nur Verschriftungen und keine Rohdaten der Session gelöscht werden.

Überwachung mehrerer Targets (z.B. AR8.2ff.): Auch hierzu finden sich keine Hinweise im BÜPF / VÜPF. Es ist anzunehmen, dass hierfür ein entsprechender Hinweis in der Verfügung der Staatsanwaltschaft vorhanden sein muss. Der Lösungsweg im ISS sollte dokumentiert und anschliessend auf Konformität geprüft werden.

Geo-bezogene Echtzeit-Alarmierung (AR8.2): Zu diesem Thema besteht heute keine Rechtsgrundlage. Eine solche ist auch im Entwurf des BÜPF nicht ersichtlich.

Geo-bezogene Alarmierung mehrerer Targets (AR8.3) sowie AR9.2ff bzgl. mehrerer Targets: Zu diesem Thema besteht heute keine Rechtsgrundlage. Eine solche ist auch im Entwurf des BÜPF nicht ersichtlich.

Sprecher Vergleichen (AR 9.1): Zu diesem Thema besteht heute keine Rechtsgrundlage. Eine solche ist auch im Entwurf des BÜPF nicht ersichtlich.

Mehrfachlogin (K4.2): Der Business-Hintergrund der Anforderung ist nachvollziehbar. Es muss eine geeignete Umsetzung innerhalb der Sicherheits-Weisungen evaluiert sein. Da der Punkt in den Gesprächen nicht diskutiert worden ist, scheint eine praktikable Lösung gefunden zu sein.

Kartenauflösung (5/6) (AR8.5): Das Thema ist in den geprüften Rechtsgrundlagen nicht geregelt.

Export und Import von Daten (K5.1ff.): Die Anforderung ist sehr abstrakt und kann erst bei Konkretisierung geprüft werden. Aufgrund der jetzigen Rechtslage muss im Berechtigungskonzept geklärt sein, was ÜPF-Anwender und was StrafB-Anwender dürfen. Mit der Revision des BÜPF könnte hier ein grösserer Handlungsspielraum eröffnet werden. Insgesamt muss gewährleistet sein, dass ein Missbrauch der hochsensiblen Daten nur mit viel krimineller Energie erfolgen kann (Datenschutz und Informatiksicherheit), eine geeignete Analyse aber nicht verhindert wird.

Weiterleitung des Datenstroms (K5.7): Zu diesem Thema besteht heute keine Rechtsgrundlage.

Aktivierung von Datenfiltern (K6.1): Das Thema ist in den geprüften Rechtsgrundlagen nicht geregelt, erscheint für den ÜPF aber nicht ausgeschlossen. Eine mögliche Filterung durch die FDA müsste ggf. noch rechtlich geregelt werden.

Zukünftige Anforderungen (Langzeitarchivierung (K10.1ff.), Import & Export): Diese Themen werden in der Revision des BÜPF adressiert. Es ist aktuell jedoch völlig unklar, wie die Version aussehen wird, die am Ende der parlamentarischen Diskussion verabschiedet wird. Daher ist eine Beurteilung der Anforderungen zum aktuellen Zeitpunkt nicht möglich.

Starke Authentifizierung (WIsB): Die aus dem WIsB und den ISC-Weisungen abgeleitete starke Authentifizierung ist aufgrund der hochsensiblen Daten angebracht. (Datenschutz)

5.1.5 [Z5] Falls es Mängel gibt, wo gibt es diese?

Betrieb: Konflikt zwischen diversen Anforderungen (Pflichtenheft, Weisungen), Beispiel [10, 11] zur Ablehnung des ADB bzgl. Einsatz Antiviren-Programm im Sinne der Nicht-Zuständigkeit. Als Lösung käme eine Rolle „Informatik-Rat ISS" mit Entscheidungskompetenz in Frage.

Zusätzlich braucht es ein klares Verständnis der System-Grenzen und des Zusammenspiels FDA – ISS-Betrieb – ISS-Hersteller – BIT, damit Aufgaben und Verantwortungen klar geregelt werden können im Sinne eines schnellen und verlustfreien Datenstroms zu den Endanwendern.

5.2 Fragestellungen

5.2.1 Frage 1: Was sind die Unterschiede zwischen einer üblichen SW und HW Installation eines Überwachungssystems der Firma *** und der Installation des ISS? (Wurde die empfohlene = recommended Architektur des Lieferanten realisiert: Storage, SAN, DB, CITRIX, Applikation, Virtualisierung)

Folgende Abweichungen zu der ursprünglich in [7] empfohlenen HW-Installation konnten identifiziert werden:

- Verwendung von iSCSI und NFS statt EMC Fibre Channel
- Verwendung von AMD- statt Intel-Prozessoren

Folgende Abweichungen zu den üblichen Anforderungen der Lösung konnten identifiziert werden:

- Keine Wartungsfenster.
- Kein Datenverlust
- 99.8% Verfügbarkeit

5.2.2 Frage 2: Welche Unterschiede führen zu den auftretenden Performance und Qualitätsproblemen?

Diese Frage wurde durch folgende Szenarien ausdetailliert, welche im Folgenden nun einzeln beantwortet werden.

[P1] Vorspulen im Gespräch erst möglich nach vollständigem Laden in Kombination mit einer langsamen Ladedauer des Gesprächs

Die Daten werden sequentiell geladen, ein Vorspulen ist daher erst möglich sobald alle Daten bis zu diesem Punkt geladen wurden. Eine Lösung ist daher nur mit einem grösseren Redesign möglich. Diese Anforderung ist so nicht spezifiziert. Insofern wäre ein Change-Request notwendig.

Bewertung der Auditoren: Das Fehlen dieser Funktion hat lediglich Komforteinbussen zur Folge und hat daher keinen Einfluss auf die generelle Einsatzfähigkeit des Systems.

[P2] Ruckeln bei Gesprächswiedergabe => Gespräch teilweise nicht mehr verständlich (schwer reproduzierbar, eher bei längeren Gespräche)

Gemäss Hersteller gab es Performance-Optimierungen für Citrix. Laut Aussage von Herrn Kalbermatten ist das Problem seit Ende Dezember 2012 nicht mehr vorhanden. Ein erneuter Test durch die StrafB ist noch ausstehend.

[P3] Anzahl (PS-) Sessions > 10'000..20'000 => Arbeiten mit Client nicht mehr möglich

Gemäss Hersteller gab es Performance-Optimierungen für die Darstellung der Sessions. Laut Aussage von Herrn Kalbermatten ist das Problem seit Ende Dezember 2012 nicht mehr reproduziert werden. Ein erneuter Test ist durch die StrafB noch ausstehend.

[P4] Datenexport mehrerer Sessions dauert «Stunden»

Exporte erfolgen mittels Stored Procedures. Performance hängt vom Storage und der HW-Box ab. Es gab keine konkreten Anforderungen zur Performance des Exports.

Bewertung der Auditoren: Die als unzureichend eingestufte Performance hat lediglich Komforteinbussen zur Folge und hat daher keinen Einfluss auf die generelle Einsatzfähigkeit des Systems.

[P5] Langsames Laden einzelner Seiten (z.B. Karten)

Die Kartendaten wurden damals von einem externen Server geladen. Diese wurden inzwischen auf der lokalen Disk abgelegt. Dies sollte zu einer Verbesserung der Performance geführt haben. Ein erneuter Test steht hier noch aus.

[Q1] Datenverlust bei der Aufzeichnung (LIVE ganzes Gespräch => gespeichert nur Teilgespräch)

Der Silence-Timeout war die vermutete Ursache. Dieser wurde inzwischen angepasst. Ein erneuter Test ist aktuell geplant. Die Ergebnisse lagen bei der Erstellung des Abschlussberichtes noch nicht vor.

[Q2] Fehlende oder nicht angezeigte Metadaten (z.B. wer, von, bis, wo) («manchmal» zeitliche Verzögerung von > «mehreren Stunden»)

Die HI2-Daten (Meta-Daten) werden von den FDAs getrennt von den HI3-Daten (Content) über FTP in das System geladen. Die Kombination der beiden Informationen erfolgt bei der LIVE-Beobachtung im Investigator, im Store&Forward in der Datenbank durch Stored Procedures welche über Trigger ausgelöst werden. Die Daten können erst angezeigt werden, sobald sie geliefert wurden. Da es keine rechtlichen Vorgaben mit den FDAs hierüber gibt, kann das System ebenfalls keine Laufzeiten garantieren. Dieses Problem ist auch im aktuellen System der Fall. Hier wurde ein Monitoring implementiert, welches Alarm auslöst, wenn Daten fehlen. Weiterhin wurde ein Prozess etabliert, mit dem die StrafB fehlende Daten nachträglich anfordern können.

Es gibt aktuell noch folgende offene Tickets in diesem Bereich:

- ISSTST-756 und ISSTST-772: Beide Major-Fehler sollen noch bis I26 gefixt werden.
- ISSTST-311: I - VD/ZH: Cell Informationen nicht in Event-List einblendbar.
  Dies ist ein CR, welcher erst nach der Pilotierung umgesetzt wird.

Bewertung der Auditoren: Sofern diese Funktionalität zwingend erforderlich ist, sind stärkere rechtliche Vorgaben für die FDAs zwingend notwendig. Sobald diese gegeben sind, sollte das System ein der Lage sein diese mit ausreichender Geschwindigkeit bereitzustellen. Das neue System scheint diese langsamer bereitzustellen als das aktuelle. Dies ist durch entsprechende Messungen zu verifizieren.

[Q3] «Datenbank Issues» (um immer die neue Daten angezeigt zu haben, muss die Anzahl Sessions auf «sehr hoch» gestellt werden) – warum ist dieser Workaround notwendig?

Es gab eine Änderung in den entsprechenden Stored Procedures aufgrund von Performance-Problemen bei anderen Kunden. Hierbei werden die obersten Sessions angezeigt, welche nicht zwingendermassen die zeitliche Reihenfolge wiederspiegeln. Es ist nicht möglich, dies für ISS anzupassen ohne eine erhebliche Abweichung vom Standard-Produkt zu verursachen. Der Hersteller arbeitet weiterhin an einer Lösung des Problems.

Bewertung der Auditoren: Für dieses Problem gibt es einen funktionierenden Workaround bei dem die Filterkriterien entsprechend eingeschränkt werden. Dieser Fehler hat lediglich Komforteinbussen zur Folge und hat daher keinen Einfluss auf die generelle Einsatzfähigkeit des Systems.

[Q4] Datenverlust bei Maskeneingaben (z.B. Verschriftungen)

Der Hersteller hat Probleme in diesem Bereich zugestanden und sichert die Behebung dieser zu. Weiterhin sind Massnahmen zur Automatisierung der Tests in diesem erkennbar, welche derartige Probleme frühzeitig adressieren sollten. Nach Aussage des Testmanagers ist in diesem Bereich aktuell eine deutliche Verbesserung erkennbar. Im Moment ist noch ein Major- (ISSTST-874) und ein Minor Defekt offen.

Bewertung der Auditoren: Die Massnahmen zur Verbesserung der Qualität scheinen zu greifen und der Trend ist positiv. Eine belastbare Aussage ist mit den Endergebnissen der Testphase erreichbar.

[Q5] «Freezer» => Manueller Abbruch => Issues mit Citrix Session Timeouts => s. Vorfall von Freitag letzte Woche

Nach Aussage des Testmanagers beim Interview vom 3.4.2013 war wie Ursache von diesem Problem ein Bedienungsfehler. Das System war nicht abgestürzt, sondern lediglich ein Dialog im Hintergrund.

Bewertung der Auditoren: Im Rahmen der aktuell durchgeführten Tests zeigt sich, dass das System erheblich stabiler funktioniert und momentan keine neuen Freezes aufgetreten sind. Die Massnahmen zur Verbesserung der Qualität scheinen zu greifen und der Trend ist positiv. Eine belastbare Aussage ist mit den Endergebnissen der Testphase erreichbar.

[Q6] «Neustart» (z.B. Kartenwechsel). Fehlermeldung => Bestätigung => Neustart => s. Vorfall vom 6.2. (siehe CD)

Nach Rücksprache mit dem externen Testmanager ist dieses Problem auf einen Bedienfehler zurückzuführen. Diese Aussage konnte mit den StrafB nicht verifiziert werden. Wir empfehlen das gemeinsame Testen durch Vertreter der StrafB und dem Testteam des Projekts.

[Q7] Unterschiedliches (zeitliches) Verhalten einzelner Arbeitsplätze (z.B. Person erfassen => Person in anderem Client nicht «vorhanden») => reproduzierbar und noch aktuell

Jeder Arbeitsplatz hat seinen eigenen Zugriff auf die Datenbanken. Beim Erfassen einer Person kann die Anwendung über das Konfigurationstool andere Anwendungen über eine Änderung benachrichtigen. Die Anwendungen pollen die Datenbank und sind daher zeitlich nicht synchronisiert.

Bewertung der Auditoren: Dieser Umstand hat lediglich Komforteinbussen zur Folge und hat daher keinen Einfluss auf die generelle Einsatzfähigkeit des Systems. Ein Benutzer sollte regelmässig einen Refresh der Daten auslösen (z.B. mittels Funktionstaste F9), um die aktuellen Informationen zu erhalten.

[Q8] Ausblendung der «fehlerhaften» Karten

Ein Fehler in der Kartendarstellung wird durch unterschiedliche Anzahl Zoom-Levels bei den Kacheln verursacht. Dieses Problem ist noch nicht korrigiert. Aktuell sind die entsprechenden Kartentypen noch deaktiviert.

Bewertung der Auditoren: Dieser Fehler hat lediglich Komforteinbussen zur Folge und hat daher keinen Einfluss auf die generelle Einsatzfähigkeit des Systems. Die Kartenfunktionalität war im Pflichtenheft nicht spezifiziert.

5.2.3 Frage 3: Ist das System der Firma *** für den Einsatz in CH - WAN Umfeld geeignet (QOS, Terminal Server CITRIX, Response Time)?

Ja, im generellen ist das System geeignet. Antwort Zeiten sind spezifisch zu definieren.

ISS muss mit den Bandbreiten im WAN von 50 Mbit/s pro Kanton resp. 256 Kbit/s pro Benutzer (Anforderung AS7.1) funktionieren.

5.2.4 Frage 4: Fand ein FAT (Factory Acceptance Test) und ein SAT (Site Acceptance Test) im realisierten SW und HW Umfeld statt – und was waren die Resultate?

Diese Frage wurde im Rahmen des Kickoff-Workshops aus dem Scope herausgenommen. Eine Beantwortung erfolgt daher nicht.

5.2.5 Frage 5: Ist das System der Firma *** für Echtzeitüberwachung ausgelegt und ist die LIVE-Funktion in der ursprünglichen Softwarearchitektur vorgesehen?

[L1] LIVE-Abspielen eines laufenden Gesprächs ist nicht möglich (erst nach Ende des Gesprächs) [AR4.4]

Die LIVE-Beobachtung eines Gesprächs ist grundsätzlich möglich. Das Wiedereinwählen in ein laufendes Gespräch (z.B.: nach dem Aufstarten des Clients oder nach einem Absturz) ist aktuell nicht möglich da dieses aus der Live-Call-Liste verschwindet. Hierzu gibt es einen Change Request (siehe ISSTST-584). Die Beauftragung von CRs ist momentan sistiert, daher ist nicht abzuschätzen, bis wann dieses Problem gelöst wird.

Das Gespräch kann erst abgespielt werden, wenn das Gespräch beendet wurde und die Verarbeitung des Gespräches in der Datenbank persistiert wurde. Die Kombination beider Effekte führen zu einer starken Beeinträchtigung der LIVE-Funktionalität.

Empfehlung der Auditoren: Der CR muss umgehend umgesetzt werden, um dieses Problem zu lösen.

[L2] s. Punkt 1: Verzögerung zwischen Gespräch und «Abspielen» < 2s [AR2.1]

Der Hersteller ist momentan nicht in der Lage, die Latenz im LIVE-Stream innerhalb seines Systems zu messen. Die Behauptung ist, es sind weniger als 2 Sekunden. Die subjektive Beobachtung am Demonstrationssystem des Herstellers erweckt den Eindruck, dass schon dort die Verzögerung mehr als 2 Sekunden beträgt.

Es sind momentan keine verlässlichen End-to-End-Messungen (auch über die Netze von BIT und Kanton) verfügbar.

Empfehlung der Auditoren: Instrumentierung des Systems und Messung.

[L3] Verzögerte Lieferung der Metadaten

Siehe [Q2]

5.2.6 Frage 6: Ist im System genügend Performanz vorhanden um zukünftige IP-Überwachungen im geforderten Umfang zu realisieren?

Das aktuelle System hat Begrenzungen bei der Ausleitung auf ca. 50Mbit/s pro FDA-Eingang. Weiterhin ist eine Chain auf 25 Mbit/s begrenzt (vor allem durch DB). Das System kann durch weitere Chains à 25 Mbit/s erweitert werden.

Ein Target kann nicht auf mehrere Chains verteilt werden. Sofern der Traffic aus einem Format besteht, muss er weiterhin durch einen Decoder verarbeitet werden, welcher damit den maximalen Durchsatz begrenzt. Der Durchsatz eines Decoders liegt im Bereich von 2-5 Mbit/s. Sofern der Traffic aus unterschiedlichen Formaten (z.B.: Email, P2P) besteht, kann er auf verschiedene Decoder verteilt werden, wodurch ein höherer Durchsatz möglich ist. Der Hersteller arbeitet an Lösungen, wie dieser Flaschenhals beseitigt werden kann. Eine kurzfristige Lösung ist aktuell aber noch nicht ersichtlich.

Die Anwendung ISS ist Datenbank-zentrisch gebaut, das heisst, alle verarbeiteten Input-Daten werden in die DB geschrieben, mittels einer zusätzlichen DB indexiert und von den Benutzer dort gelesen. Die Datenbanken werden durch die direkte Anbindung der Fat Clients (2-Tier-Architektur), als auch durch das Postprocessing und Archivierung belastet. Hierdurch kann nicht garantiert werden, dass genügend Leistung für die Speicherung der Input-Daten bereitsteht.

Der Durchsatz der Datenbank in den Bereichen Rechenleistung (CPU) und Speicher (I/O) muss entsprechend gewährleistet sein und für künftiges Wachstum skalieren.

Um ISS weiter zu skalieren, werden daher in der Zukunft grössere SW- und HW-Änderungen notwendig sein.

Der Hersteller arbeitet an Konzepten, wie diese Begrenzungen überwunden werden können. Der Hersteller hat hierzu eine Roadmap für seine Plattform aufgestellt. Weiterhin arbeitet der Hersteller aktuell an Offerten, wie ISS auf 50, 100 und 300 Mbit/s erweitert werden kann.

5.2.7 Frage 7:Ist das Rechenzentrum ISC-EJPD mit den Auflagen des Bundes in der Lage, ein hochkomplexes System im Bereich der Kommunikationsüberwachung für die schweizerischen StrafB zu betreiben?

Diese Frage wird ausführlich in Abschnitt 4.1.5 beantwortet. Die Gesamtbewertung orientiert sich an den problematischsten Punkten (geteilte physikalische Ressourcen und Weisungen)

5.3 Erweiterte Aufgabenstellung durch das ISC-EJPD

5.3.1 [E1] Prüfung des heute gelieferten Systems gegen das Pflichtenheft

Geprüft wurden architektonische Grundzüge und die Rechtskonformität der Anforderungen. Die Ergebnisse sind in Kapitel 4 dargestellt.

Aktuell laufen Tests zur Prüfung des gelieferten Systems, diese werden vom Projekt und nicht von den Auditoren geleistet. Von Seiten ÜPF und ISC-EJPD gibt es Signale, dass es deutliche Verbesserungen gibt. Eine abschliessende Beurteilung durch das Projekt liegt noch nicht vor.

5.3.2 [E2] Prüfung des Systems auf Erfüllung der heutigen Rechtsgrundlagen

5.3.2.1 Überwachungstyp CS

[Ü1] Echtzeit-Überwachung der Nutzinformationen

Diese Daten können übertragen werden. Es gibt die in Abschnitt 4.1.3 erwähnten Einschränkungen hinsichtlich Latenz bei der LIVE-Beobachtung.

[Ü2] bei Mobiltelefonie: Echtzeit-Überwachung

Diese Daten können übertragen werden. Es gibt die in Abschnitt 4.1.3 erwähnten Einschränkungen hinsichtlich Latenz bei der LIVE-Beobachtung.

[Ü3] Echtzeit-Überwachung: auch bei Nicht-Aufbau der Kommunikation müssen Angaben bereitgestellt und simultan oder periodisch übertragen werden

Diese Informationen werden übertragen.

[Ü4] Suche vermisster Personen: Echtzeit-Verkehrsdaten inkl. Standort

Dies entspricht aus technischer Sicht Ü2 und Ü3.

5.3.2.2 Überwachungstyp Internet (PS)

[Ü5] Überwachung eines Internetzugangs (Echtzeit)

Alle Daten des Internetzugangs können überwacht werden. Das System hat allerdings im Worst-Case eine zu geringe Verarbeitungskapazität von ca. 2-5 Mbit/s pro Target. Dies ist momentan nicht ausreichend, um einen Anschluss mit bis zu 100 Mbit/s zu überwachen.

[Ü6] Bereitstellung und simultane oder periodische Übermittlung von Angaben über den Internetzugang (Echtzeit)

Diese Daten stehen prinzipiell zur Verfügung. Die Einschränkungen aus [Ü5] gelten allerdings auch hier.

[Ü7] Übertragung der Nutzinformationen der überwachten Anwendung (Echtzeit)

In den PR-Anforderungen der Funktionsliste [2] sind die zu überwachenden Anwendungen genauer spezifiziert. Die meisten sind entweder schon im Standardprodukt enthalten oder wurden nachimplementiert. Folgende Anforderungen waren zum 2.7.2012 noch nicht realisiert, sollten aber bis Ende 2012 umgesetzt sein. Der aktuelle Stand ist nicht beurteilbar und muss durch entsprechende Systemtests verifiziert werden.

- PR 2.4 SSH Secure Shell
- PR 3.2 ARCOR
- PR 3.4 Bluewin Mail
- PR 3.41 Swissmail
- PR 3.46 Web.de
- PR 3.48 YA (ES)
- PR 3.50 ZZN
- PR 4.25 JUBII (DE, COM)
- PR 4.41 TERRA
- PR 6.1 VoIP call content (6/8) G.729B
- PR 6.3 VoIP signalling (2/3) H.450
- PR 6.8 iSpQ
- PR 7.13 T.38

[Ü8] Bereitstellung und simultane oder periodische Übermittlung von Kommunikationsparametern aus der Überwachung einer Anwendung (Echtzeit)

Genauere Spezifikationen, welche Kommunikationsparameter pro Anwendung bereitgestellt werden sind nicht vorhanden. Daher erfolgt hier keine separate Bewertung.

5.3.3 [E3] Prüfung des Systems auf mögliche Erfüllung der künftigen Rechtsgrundlagen

Langzeitarchivierung, Datenimport oder –Export und Schnittstellen

Diese Funktionalitäten können nur mittels speziell implementierten Stored Procedures auf der Datenbank realisiert werden. Da es noch keine genaueren Anforderungen in diesem Bereich gibt, ist nicht abzuschätzen, inwieweit die im Standardprodukt enthaltenen Ansätze ausreichend sind. Die Schnittstelle ist insgesamt nicht sehr flexibel und erfordert Implementierungsaufwand durch den Hersteller, um die Anforderungen umzusetzen.

Kritisch ist hier die zusätzliche Belastung der Datenbank zu sehen. Inwiefern dies allerdings tatsächliche Auswirkungen auf die Gesamtperformanz des Systems hat, kann aktuell noch nicht abgeschätzt werden.

5.3.4 [E4] Ist das System technisch reif für einen derartigen Einsatz?

Die Güte des Systems muss durch Tests geprüft werden. Diese sind aktuell in der Durchführung, allerdings noch nicht abgeschlossen. Die Stabilisierungsmassnahmen scheinen zu greifen, ob sich dieser Trend fortsetzen wird, kann erst im Laufe der Pilotierung bestimmt werden.

Grundsätzlich ist die Architektur des Systems ausreichend, um die Anforderungen des Pflichtenhefts zu ermöglichen.

Im Bereich PS ist die Redundanz noch nicht gewährleistet. Ein entsprechendes Konzept ist aktuell in Arbeit und kann daher nicht abschliessend beurteilt werden.

Die Skalierbarkeit im Bereich PS ist momentan noch nicht ausreichend gewährleistet. Details sind in Abschnitt 5.2.6 beschrieben.

5.3.5 [E5] Hat der Hersteller die geeigneten Kapazitäten bei der Entwicklung?

Ja, der Hersteller hat genügend Kapazitäten. Ebenfalls ist die technische und fachliche Expertise in ausreichendem Masse vorhanden. Die Übernahme durch einen Grosskonzern hat die Entwicklungskapazitäten sogar noch stark vergrössert, sodass diese auch in Zukunft gesichert sind.

Der Entwicklungsprozess inklusive Branch-Strategie und Testing wurde deutlich verbessert.

5.3.6 [E6] Verfügt das System über Schnittstellen für eine zukünftige Erweiterung?

Siehe 5.3.3

5.3.7 [E7] Welche Ansätze gibt es für eine Langzeitarchivierung?

Siehe 5.3.3

6. Anhang

6.1 Auftrag zum System-Audit ISS

Der Leiter des ISC-EJPD hat Zühlke mit dem System-Audit ISS beauftragt.

Gemäss Auftrag sind im Rahmen des System-Audits folgende Fragen zu klären:

1. Was sind die Unterschiede zwischen einer üblichen SW- und HW-Installation eines Überwachungssystems der beauftragten Firma (Hersteller) und der Installation des ISS? (Wurde die empfohlene = recommended Architektur des Lieferanten realisiert: Storage, SAN, DB, CITRIX, Applikation, Virtualisierung)
2. Welche Unterschiede führen zu den auftretenden Performance und Qualitätsproblemen?
3. Ist das System des Herstellers für den Einsatz in CH - WAN Umfeld geeignet (QOS, Terminal Server CITRIX, Response Time)?
4. Fand ein FAT (Factory Acceptance Test) und ein SAT (Site Acceptance Test) im realisierten SW und HW Umfeld statt – und was waren die Resultate?
5. Ist das System des Herstellers für Echtzeitüberwachung ausgelegt und ist die LIVE Funktion in der ursprünglichen Softwarearchitektur vorgesehen?
6. Ist im System genügend Performanz vorhanden, um zukünftige IP-Überwachungen im geforderten Umfang zu realisieren?
7. Ist das Rechenzentrum ISC-EJPD mit den Auflagen des Bundes in der Lage, ein hochkomplexes System im Bereich der Kommunikationsüberwachung für die schweizerischen StrafB zu betreiben?

Zur Schärfung des Scopes werden beim Kickoff die Erwartungen erfragt. Teilnehmer des Kickoffs waren [redacted] sowie die Auditoren Zühlke.

6.1.1 Schärfung des Auftrags: Erwartungen und Ziele gemäss Kickoff-Workshop

Auf breiter Basis stand die Frage der Teilnehmer: **„Werden die Anforderungen der StrafB vom System erfüllt?"** Einhellig wurde ein System-Audit im Sinne eines **„fit for purpose"** beschlossen.

Als Ziel wurde formuliert:

[Z1] Wie soll mit ISS fortgefahren werden: sanieren, portieren oder neu evaluieren?

Die Teilnehmer erhoffen sich eine Entscheidungshilfe für konkrete Massnahmen vom Audit.

6.1.2 Scope-Erweiterung gemäss Kickoff

Bei Einzelbetrachtung der 7 Fragen des Auftrags wurde zwar die Streichung der Frage 4, insgesamt aber eine deutliche Scope-Erweiterung gegenüber dem Angebot beschlossen.

Scope gemäss Angebot	Scope gemäss Kickoff
Anhand der Frageliste wird das System geprüft. Die Findings werden in einer Deltaliste festgehalten und anschliessend ausgewertet.	Anhand der überarbeiteten Frageliste (Szenarien) wird das System geprüft. Die Findings werden in einer Deltaliste festgehalten und anschliessend ausgewertet. Zusätzlich wird um ein Referenzsystem des Herstellers gebeten. Das ISS-System wird anhand der Szenarien gegen das Referenzsystem geprüft. Die Findings werden in einer Deltaliste festgehalten und anschliessend

	ausgewertet. Der Bericht liefert eine Entscheidungsgrundlage für konkrete Massnahmen.

Dieser deutlich erweiterte Scope ist bei gleichem Aufwand nur machbar, wenn die Anzahl der zu prüfenden Szenarien so gering wie möglich gehalten werden kann.

Die Prüfung des Referenzsystems ist nur bei enger Kooperation des Herstellers möglich. Es ist Aufgabe des ISC-EJPD, Verhandlungen und Incentivierung zur Kooperation durchzuführen und eine Machbarkeit dieser gewünschten Audit-Aufgaben sicherzustellen.

Die Prüfung des Pflichtenhefts gegen das System ist nicht Bestandteil des System-Audits. Basis für das System-Audit werden Szenarien sein, die mit den StrafB im Rahmen eines Workshops am 25.2.2013 in Zürich erarbeitet werden. Aus Sicht ÜPF / ISC bedarf es keiner speziellen ÜPF-Szenarien.

6.1.3 Szenarien-WS vom 25.02.2013

Die Szenarien sollen helfen, den Kontext einer Anforderung einzubeziehen und darin auftauchende Probleme (Performance oder Qualität) gezielter zu hinterfragen. Die Fragen 1-3 sowie 5-7 bleiben relevant fürs Audit.

Ausgehend von Frage 2 und 5 wurden folgende Szenarien zu Performance [P], zu Qualität [Q] und zur LIVE-Überwachung [L] definiert (siehe auch Protokoll des Szenarien-WS, die Reihenfolge entspricht der Priorität):

- [P1] Vorspulen im Gespräch erst möglich nach vollständigem Laden in Kombination mit einer langsamen Ladedauer des Gesprächs
- [P2] Ruckeln bei Gesprächswiedergabe => Gespräch teilweise nicht mehr verständlich (schwer reproduzierbar, eher bei längeren Gespräche)
- [P3] Anzahl (PS-) Sessions > 10'000..20'000 => Arbeiten mit Client nicht mehr möglich
- [P4] Datenexport mehrerer Sessions dauert «Stunden»
- [P5] Langsames Laden einzelner Seiten (z.B. Karten)
- [Q1] Datenverlust bei der Aufzeichnung (LIVE ganzes Gespräch => gespeichert nur Teilgespräch)
- [Q2] Fehlende oder nicht angezeigte Metadaten (z.B. wer, von, bis, wo) («manchmal» zeitliche Verzögerung von > «mehreren Stunden»)
- [Q3] «Datenbank Issues» (um immer die neue Daten angezeigt zu haben, muss die Anzahl Sessions auf «sehr hoch» gestellt werden) – warum ist dieser Workaround notwendig?
- [Q4] Datenverlust bei Maskeneingaben (z.B. Verschriftungen)
- [Q5] «Freezer» => Manueller Abbruch => Issues mit Citrix Session Timeouts => s. Vorfall von Freitag letzte Woche
- [Q6] «Neustart» (z.B. Kartenwechsel). Fehlermeldung => Bestätigung => Neustart => s. Vorfall vom 6.2. (siehe CD)
- [Q7] Unterschiedliches (zeitliches) Verhalten einzelner Arbeitsplätze (z.B. Person erfassen => Person in anderem Client nicht «vorhanden») => reproduzierbar und noch aktuell
- [Q8] Ausblendung der «fehlerhaften» Karten
- [L1] LIVE-Abspielen eines laufenden Gesprächs ist nicht möglich (erst nach Ende des Gesprächs) [AR4.4]
- [L2] s. Punkt 1: Verzögerung zwischen Gespräch und «Abspielen» < 2s [AR2.1]
- [L3] Verzögerte Lieferung der Metadaten (siehe auch Q2)

Die Reihenfolge der Szenarien entspricht ihrer Priorität. Prio 1-3 sollten abgedeckt werden, die weiteren Szenarien nur nach Möglichkeit und nach „Best-Effort"-Prinzip.

6.1.4 Erweiterte Aufgabenstellung durch das ISC-EJPD

Zusätzlich zu den im ursprünglichen Umfang vorgesehenen Aufgaben sollen in der Erweiterung des Auftrages durch das ISC-EJPD die folgenden Punkte untersucht werden:

- [E1] Prüfung des heute gelieferten Systems gegen das Pflichtenheft
- [E2] Prüfung des Systems auf Erfüllung der heutigen Rechtsgrundlagen
- [E3] Prüfung des Systems auf mögliche Erfüllung der künftigen Rechtsgrundlagen
- [E4] Ist das System technisch reif für einen derartigen Einsatz
- [E5] Hat der Hersteller die geeigneten Kapazitäten bei der Entwicklung
- [E6] Verfügt das System über Schnittstellen für eine zukünftige Erweiterung
- [E7] Welche Ansätze gibt es für eine Langzeitarchivierung

Das Ziel des Zusatzauftrages ist, Folgendes abzuklären:

- [Z2] Hat der Lieferant das geliefert, was er angeboten hat? (Teile des Angebotes können sich von den Anforderungen unterscheiden. Beispielsweise wenn im Angebot steht, dass eine geforderte Funktionalität nur mit der Erweiterung des System erreicht werden kann.)
- [Z3] Kann der Lieferant ein lauffähiges System liefern?
- [Z4] Gegenüberstellung von Rechtsgrundlagen und Anforderungen: Decken die Anforderungen die Rechtsgrundlagen ab? (Grundsätzlich müssten das Pflichtenheft die aktuellen Rechtsgrundlagen abdecken. Die zukünftigen Rechtsgrundlagen werden möglicherweise nur teilweise abgedeckt.)
- [Z5] Falls es Mängel gibt, wo gibt es diese?

Der Abgabetermin des Berichtes verschiebt sich gegenüber dem im Grundauftrag erwähnten Termin (18.3.2013) auf den 5.4.2013. Im Anschluss sollen Ergebnisse des Reviews in zwei Präsentation vorgestellt werden. Die genauen Termine für die Präsentation sind noch zu definieren.

Die Ziele und Erwartungen sowie die Scope-Schärfung werden wiederum in einem Kickoff-Workshop erarbeitet.

Die Ergebnisse sowie das Vorgehen werden in einer aktualisierten Version dieses Dokuments festgehalten.

6.1.5 Relevante Rechtsgrundlagen

Die relevanten Rechtsgrundlagen bezüglich Fernmeldeüberwachung:

- Bundesgesetz http://www.admin.ch/ch/d/sr/c780_1.html (Art. 13)
- Verordnung zum Bundesgesetz http://www.admin.ch/ch/d/sr/c780_11.html (Art. 7-10; Art. 16-18; Art. 24)
- Gebührenverordnung http://www.admin.ch/ch/d/sr/c780_115_1.html
- Strafprozessordnung http://www.admin.ch/ch/d/sr/c312_0.html (Relevant Art. 269 - 279)
- Revisioniertes BÜPF (in Überarbeitung, Draft per Email zugestellt)
- Statusbericht Rechtsetzungsverfahren (20.6.2011) und bewertete Funktionsliste (zugestellt per Email durch [redacted])

Die relevanten Rechtsgrundlagen zur Informatik im EJPD:

- Weisung über die Informatik im Eidg. Justiz- und Polizeidepartement (Informatikweisung EJPD)
- Weisung des EJPD über die Umsetzung des Datenschutzes und der Informationssicherheit (DSIS-Weisung EJPD).
- Weisungen des IRB über die Informatiksicherheit in der Bundesverwaltung (WIsB)

- Sicherheitsweisungen ISC-EJPD, z.B. Nummer 03, 10

6.1.6 Erwartungen und Ziele gemäss Kickoffs zum Erweiterungsauftrag

Leitfrage des System-Audits: Ist der Hersteller in der Lage, ein lauffähiges System zu liefern?

6.1.7 Scope-Erweiterung

Aufgaben aus der Erweiterung des Audits

- Prüfung der Rechtskonformität: Schwerpunkt sind die geforderten Überwachungstypen. Kann das ISS die Überwachungstypen entgegennehmen und verarbeiten?
- Weitere Themen aus der Revision BÜPF: Langzeitspeicherung, Import & Export
- Prüfen des Pflichtenhefts gegen das System: Schwerpunkt liegt auf AR- und K-Anforderungen. (WMS ist nicht im Scope, da dies eine Individualentwicklung ist.)
- Weisungen des ISC und des Department /BR können im Rahmen der Frage 7 (Kapitel 2.1) relevant.

6.1.8 Vorgehen zum System-Audit

- Kurze Projekt-Einführung durch PL ISS
- Interviews Architekt / Betrieb ISC
- Workshop mit StrafB: Erarbeitung der Szenarien (25.2.2013)
- Sichtung relevanter Dokumente sofern erwünscht und nützlich
- Klärung des Rechtskontexts mit den Juristen des ÜPF
- Klärung der Ableitung von Anforderungen aus den relevanten Weisungen für den Betrieb mit [redacted]
- 2-tägiger Workshop beim Hersteller
- Interview Testmanager ISS
- Auswertungen des Workshops und des Dokumentenstudiums im Bericht (Draft-Version bis 5.4.2013)
- Abschlussbericht (12.4.2013) und Präsentation Präsentation im LG FMÜ am 24.4.2013

6.2 Interviews und Workshops mit Teilnehmern

Folgende Teilnehmer haben die Auditoren tatkräftig bei der Informationssammlung und Sichtung unterstützt:

- StrafB: [redacted]
- ISC-EJPD / ÜPF: [redacted] (Auftraggeber des Audits), [redacted]
- Hersteller: Projektleiter (aktueller und ehemaliger), System Consultant, diverse Spezialisten und Lead Developer

Vielen Dank für Ihre wertvolle Unterstützung!