EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
CONTROLLA FEDERALA DA FINANZAS

Informatikstrategieorgan Bund (ISB)

Prüfung im Bereich der Informatikstrategie Bund

21. Oktober 2009

Inhaltsverzeichnis

Abkürzungsverzeichnis und Glossar

ABB	Architektur Board Bund
Admin-PKI	Public Key Infrastructure Lösung des BIT für administrative IT-Anwendungen
A-IS	Ausschuss Informatik-Sicherheit
BinfV	Bundesinformatikverordnung
BIT	Bundesamt für Informatik und Telekommunikation
BR	Bundesrat
BSC	Balanced Score Card
BVerw	Bundesverwaltung
CMMI	Capability Maturity Model Integrated
COBIT	**C**ontrol **Ob**jectives for **I**nformation and Related **T**echnology. International anerkannter Standard für IT-Governance: Synthese von insgesamt 41 nationalen und internationalen Standards aus den Bereichen Kontrolle, Sicherheit, Qualitätssicherung und IT
Commodity	Handelsware (z.B. Gold, Eisen, Oel, usw.). Bezogen auf den Bund auch als Begriff für „Bundesweite Standarddienste und –produkte“ bzw. Services verwendet.
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
EFV	Eidgenössische Finanzverwaltung
FBB	Führung Forest Bund
FinDel	Finanz Delegation
FUB	Führungsunterstützungsbasis, Supportorganisation des VBS im IT-Bereich
GL	Geschäftsleitung
GS	Generalsekretär / Generalsekretariat
GSK	Generalsekretären-Konferenz
HERMES	Projektführungsmethode zum Führen und Abwickeln von IKT-Projekten; offener Standard der BVerw, der u.a. in den Kantonen eingesetzt wird (www.hermes.admin.ch.)
ICO	Informatik-Controlling
IKT	Informations- und Kommunikationstechnologie(n)
IRB	Informatikrat Bund
ISB	Informatikstrategieorgan Bund
ISBO	Informatiksicherheitsbeauftragter der Organisation
IT	Informationstechnologie; Informatik
IT-Governance	Integraler Bestandteil der Corporate Governance. Liegt in der Verantwortlichkeit des Verwaltungsrates und der GL. IT-Governance besteht aus Führung sowie organisatorischen Strukturen und Prozessen, die sicherstellen, dass die IT die Geschäftsabläufe und -ziele der VE effizient und effektiv unterstützt.
ITIL	Information Technology Infrastructure Library
LBK	Leistungsbezügerkonferenz
LB	Leistungsbezüger
LE	Leistungserbringer
NOVE-IT	Reorganisation der Bundesinformatik
OE	Organisationseinheit(en)
PAB	Prozessausschuss Bund
PCO	Projektcontrolling, PCO-Bericht gemäss Vorgaben NOVE-IT (Teil des ICO)
PKI	Public Key Infrastructure
PL	Projektleitende, -leitung
SAP-R/3	SAP Release 3, betriebswirtschaftliche Anwendung
SD-PKI	SwissDefence-Public Key Infrastructure Lösung des VBS
SIP	Strategische Informatikplanung
SLA	Service Level Agreement
SOA	Service Oriented Architecture
TOGAF	The Open Group Architecture Framework
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VE	Verwaltungseinheit(en)

1 Zusammenfassung des Prüfungsbefundes

Die Hauptziele dieser Revision beim Informatikstrategieorgan Bund (ISB) bildeten einerseits die Prüfung der Umsetzung des Bundesrats-Auftrages vom Mai 2007 welcher vorsieht, im Rahmen des Informatikrates Bund (IRB) Rolle, Aufgabe und Zusammensetzung der IKT-Führungsgremien und IKT-Stabsorganisationen der Bundesverwaltung zu überprüfen und dem Bundesrat (BR) allfällige Anpassungen innert Jahresfrist zu beantragen sowie weitere Prüfungsbereiche. Dazu gehören Abklärungen, wie die Überwachung der IKT-Strategie erfolgt, welche Instrumente und Strukturen zur Durchsetzung von Normen sowie Standards bestehen, ob diese Normen und Standards eingehalten werden und ob Synergiepotenziale bzw. Doppelspurigkeiten vorhanden sind. Ein Spezialgebiet betraf die Abklärung bezüglich Umsetzung der Public Key Infrastructure (PKI) beim VBS und beim Bundesamt für Informatik (BIT). Zusätzlich wurde der aktuelle Stand aus den früheren Revisionen 5037_Budgetprozess IT Invest EFD, 5039_Org & Aktivität ISB, 7296_QP KNW bei IKT-Grossprojekten und 7402_SAP-Strategie eruiert.

Gesamtheitlich beurteilt die Eidgenössische Finanzkontrolle (EFK) die Prüfungsergebnisse in dem Sinne, dass der Bundesrats-Auftrag noch nicht umgesetzt ist, dass die Einhaltung der IKT-Strategie und definierten Normen und Standards nur teilweise aktiv überwacht wird und noch Synergiepotenziale bestehen. Daher empfiehlt die EFK im Rahmen ihrer Prüfungen im Wesentlichen dem ISB via IRB,

- eine Grundsatzentscheidung, ob der Geltungsbereich der BinfV gemäss Art. 2 für das VBS aufgrund dessen IKT-Strategie geändert oder präzisiert werden muss. Insbesondere gilt es zu klären, ob die für die Einsatzsysteme der Armee vorgesehene Ausnahme auf das ganze VBS auszudehnen ist und wie in einem solchen Fall die Effizienz und Interoperabilität über die ganze Bundesverwaltung sichergestellt werden kann,
- alle Studien, Projekte und Anwendungen aller Departemente und der Bundeskanzlei auf Stufe Bund im IKT-Cockpit zu integrieren,
- möglichst vollständige und genaue Datenlieferungen seitens der Leistungserbringer (LE) und betroffenen Departemente hinsichtlich IT-Kosten zu erwirken und diese in die Balanced Score Card (BSC) einfliessen zu lassen,
- die Aufgaben des IRB (gemäss BinfV Art. 13, Abs. 2 Buchstabe a) betreffend der Überwachungsfunktion wo nötig zu präzisieren und konsequenter umzusetzen, was die Einhaltung der Informatikvorgaben betrifft,
- einen Umsetzungsplan für die Motion Noser (Nr. 07.3452) mit dem Ziel zu erstellen, eine Konzentration auf möglichst wenige oder nur noch einen Leistungserbringer zu erreichen und dabei die Grundsatzentscheidung, wie weit das VBS dem Geltungsbereich der BinfV zukünftig noch unterliegt (siehe oben), zu berücksichtigen,
- eine SLA-Standardisierung für Betrieb und Unterhalt von IT-Anwendungen und der Büroautomation anzustreben, mittels derer ein Leistungserbringer vergleichbare und transparent dargelegte Kosten offerieren muss. Dabei ist auch auf die Einhaltung internationaler Standards – wie z.B. ITIL, Einhaltung der IT-Sicherheitsorganisation gemäss ISO 27001, usw. – zu achten. Dies gilt vor allem für sogenannte Commodities, d.h. für bundesweit verwendete Standarddienste und –produkte bzw. Services im Bereich der IT.

Auf dem Spezialgebiet der Public Key Infrastructure (PKI) wurde beim VBS die angestrebte Lösung einer SwissDefence-PKI (SD-PKI) mit der Admin-PKI des Bundesamt für Informatik (BIT) verglichen und ein unabhängiger Teilbericht durch die EFK [siehe **Beilage 5**] erstellt. Zusammenfassend erachtet es die EFK aus technischer wie auch aus sicherheitsbezogener Sicht noch nicht als zwingend nachgewiesen, dass das VBS eine eigene SD-PKI realisieren und betreiben muss. Der IRB hat an der Sitzung vom 25. Mai 2009 das diesbezügliche Ausnahmegesuch des VBS zur Realisierungen einer eigenen SD-PKI nicht definitiv akzeptiert, sondern nur einen zweijährigen Versuchsbetrieb bewilligt. Bis zum Juni 2010 sollen das VBS und das BIT einen Vorschlag erstellen, inwieweit eine einheitliche Public Key Infrastructure auf die Bundesverwaltung bezogen durch den Bund betrieben werden kann und wie diese zwei PKI-Lösungen zusammengeführt werden. Die Verantwortlichen des VBS haben zu den Feststellungen und Empfehlungen im Detailbericht SD-PKI [siehe **Beilage 5**] eine andere Sichtweise und sind in wesentlichen Teilen damit nicht einverstanden. Die kontrovers geführten Diskussionen betreffend PKI zwischen VBS und IRB bzw. ISB oder dem BIT werden aus Sicht des VBS behindert, weil vorgängig generelle Entscheidungen auf Stufe Bund über die Steuerung Führung der IT zu treffen wären. Für weitere Details verweisen wir auf Kapitel 3.6 und **Beilage 5.**

Infolge anderer Prioritätensetzung seitens der EFK wurde nur der Umsetzungsstand und der Status für die im Zuge der früheren Prüfungen (5037_Budgetprozess IT Invest EFD, 5039_Org & Aktivität ISB, 7296_QP KNW bei IKT-Grossprojekten und 7402_SAP-Strategie) abgegebenen Empfehlungen und vorgesehenen Massnahmen aus Sicht des ISB erhoben.

2 Auftrag und Prüfungsdurchführung

2.1 Auftrag

Gestützt auf die Artikel 6 und 8 des Finanzkontrollgesetzes (FKG; SR 614.0) hat die Eidgenössische Finanzkontrolle (EFK) von Anfang April bis Mitte Juli 2009 Prüfungen im Bereich Informatikstrategie beim ISB durchgeführt.

2.1.1 Prüfungsziel

Diese Prüfung wurde mit dem hauptsächlichen Ziel durchgeführt, ob die Informatikstrategie in der Bundesverwaltung wirksam ist und im Sinne der strategischen Vorgaben umgesetzt wird.

2.1.2 Schwerpunktfragen

Die folgenden Detailfragen sollen beantwortet werden:

- Welches ist der Stand der vom BR im Mai 2007 dem EFD in Auftrag gegebenen Überprüfung der Rolle, Aufgabe und Zusammensetzung der IKT-Führungsgremien und IKT-Stabsorganisationen der BVerw?
- Besteht ein wirksames Instrument zur laufenden Überwachung und periodischen Beurteilung, ob die IKT-Strategie des Bundes erfolgreich umgesetzt wird?
- Verfügt der IRB / das ISB bzw. die Bundesverwaltung über die notwendigen Instrumente und Strukturen, um die festgelegten Normen und Standards durchzusetzen?
- Wie beurteilt der IRB / das ISB die Einhaltung der geltenden Bundesstandards durch die Departemente?
- Nimmt der IRB (das ISB) dabei seine strategische Verantwortung angemessen wahr?
- Wird im Sinne der IKT-Strategie des Bundes verfahren / gehandelt?
- Wird das Synergiepotenzial weitestgehend genutzt (finanziell, technologisch) und werden Doppelspurigkeiten soweit möglich verhindert?
- Spezialthema Public Key Infrastructure (PKI): Entspricht die aktuelle Situation den strategischen Vorgaben?
- Wurden die Empfehlungen / vorgesehenen Massnahmen (oder allenfalls andere zielführende Massnahmen im Sinne der Empfehlungen) aus früheren Revisionen 5037, 5039, 7296, 7402 umgesetzt?

2.2 Rechts- und Revisionsgrundlagen sowie Vorgabedokumente

Allgemein

- Bundesgesetz über die Eidgenössische Finanzkontrolle vom 28. Juni 1967 (Stand am 1. Januar 2009), SR 614.0,
- Bundesgesetz über den eidgenössischen Finanzhaushalt (Finanzhaushaltgesetz, FHG) vom 7. Oktober 2005 (Stand 1. Januar 2009), SR 611.0,
- Finanzhaushaltverordnung (FHV) vom 5. April 2006 (Stand am 1. Januar 2009), SR 611.01,
- Informatikprozesse der Bundesverwaltung (P01 – P09) (intranet.informatikprozesse.isb.admin.ch),
- ITIL (IT Infrastructure Library)[1] der OGC (The Office of Government Commerce) in Norwich (England),
- CobiT[2]-Framework, Version 4 vom Juli 2005.

Informatikstrategieorgan Bund

- Regierungs- und Verwaltungsorganisationsgesetz (RVOG) vom 21. März 1997 (Stand am 1. Januar 2009), SR 172.010,
- Regierungs- und Verwaltungsorganisationsverordnung (RVOV) vom 25. November 1998 (Stand 1. Juli 2009), SR 172.010.1,
- Art. 8 der Organisationsverordnung vom 11. Dezember 2000 für das Eidgenössische Finanzdepartement (OV-EFD; Stand am 1. Januar 2009), SR 172.215.1,
- Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV) vom 26. September 2003 (Stand am 1. Januar 2009), SR 172.010.58,
- Verordnung über die Organisation des öffentlichen Beschaffungswesens des Bundes (Org-VoeB) vom 22. November 2006 (Stand am 27. Dezember 2006), SR 172.056.15,
- Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens vom 17. Oktober 2007.

2.3 Prüfungsumfang und -grundsätze

Die Prüfung bezog sich auf die unter Ziffer 2.1 erwähnten Ziele und Schwerpunkte. Die Prüfungshandlungen erfolgten - unter Berücksichtigung der im vorstehenden Abschnitt aufgeführten Rechtsgrundlagen und Vorgabedokumente - nach anerkannten Revisionsgrundsätzen. Die Beurteilung des IKT-Potenzials auf Basis von CobiT ist ein wesentlicher Teil der Umsetzung der IT-Governance. Die dazugehörigen Schlüsselfragen lauten:

- Ist die IKT auf das Kerngeschäft ausgerichtet?
- Unterstützt die IKT das Geschäft und maximiert sie den Nutzen?
- Wird mit den IKT-Ressourcen verantwortungsbewusst umgegangen?
- Werden IKT-Risiken angemessen gemanagt? Wird die IT-Governance gelebt und gemessen?

Die Abbildung in **Beilage 1** beschreibt kurz die fünf Kernbereiche der IT-Governance.

---

[1] ITIL®: De-facto-Standard im Bereich Servicemanagement, beinhaltet eine umfassende und öffentlich verfügbare fachliche Dokumentation zur Planung, Erbringung und Unterstützung von IT-Servicedienstleistungen; www.ogc.gov.uk oder www.itil.co.uk .

[2] CobiT®, Governance, Control and Audit for Information and Related Technology, 4rd Edition, www.ITgovernance.org und www.isaca.org.

Einzelheiten über Art und Umfang der durchgeführten Prüfungen gehen aus unseren Arbeitspapieren hervor.

2.4 Unterlagen und Auskunftserteilung

Die gewünschten Unterlagen standen uneingeschränkt zur Verfügung. Die notwendigen Auskünfte wurden dem Revisionsteam zuvorkommend und kompetent erteilt.

2.5 Priorisierung der Empfehlungen der EFK

Aus der Sicht des Prüfauftrages beurteilt die EFK die Wesentlichkeit der Empfehlungen und Bemerkungen nach Prioritäten (1 = hoch, 2 = mittel, 3 = klein). Sowohl der Faktor **Risiko** [z.B. Höhe der finanziellen Auswirkung bzw. Bedeutung der Feststellung; Wahrscheinlichkeit eines Schadeneintrittes; Häufigkeit des Mangels (Einzelfall, mehrere Fälle, generell) und Wiederholungen; usw.], als auch der Faktor **Dringlichkeit der Umsetzung** (kurzfristig, mittelfristig, langfristig) werden berücksichtigt.

3 Detailergebnisse der Überprüfung Informatikstrategieorgan Bund (ISB)

3.1 Die Überprüfung der Rollen, Aufgaben und die Zusammensetzung der IKT-Führungsgremien und IKT-Stabsorganisationen der Bundesverwaltung ist noch nicht umgesetzt

Der Auftrag des Bundesrates erfolgte im Rahmen einer Anpassung der Bundesinformatikverordnung (BinfV) vom 1. Mai 2007, anlässlich derer ein Wechsel des Vorsitzes im Informatikrat Bund (IRB) beschlossen wurde. Dabei wurde das EFD beauftragt, im Rahmen des IRB Rolle, Aufgabe und Zusammensetzung der IKT-Führungsgremien und IKT-Stabsorganisationen der Bundesverwaltung zu überprüfen und dem Bundesrat allfällige Anpassungen innert Jahresfrist zu beantragen. Im Herbst 2007 wurde damit begonnen, mit dem Ziel, im Frühjahr 2008 den Auftrag erfüllt zu haben. In Beantwortung eines Schreibens der Finanzkommission des Nationalrates wurde darauf hingewiesen, dass die Umsetzung des BR-Auftrages im Rahmen der Motion 05.3470 aufgenommen wird. Wegen der Finanzkrise und der Diskussion um das Bankgeheimnis haben sich die Prioritäten verschoben und ein Grundsatzentscheid über die Umsetzung des BR-Auftrages ist noch nicht erfolgt. Seit Januar 2009 sind die Arbeiten – als interdepartementale Diskussion auf Generalsekretären-Ebene – wieder angelaufen.

Innerhalb des Eidgenössischen Finanzdepartements (EFD) bestehen hinsichtlich IKT-Führungsgremien verschiedene Rollen. Dabei gibt es eine Rolle Gesamt IKT-Steuerung mit dem IRB und dessen Stabsorgan ISB (vgl. **Beilage 2** – Organisation des ISB); eine Rolle als Leistungserbringer (LE), darunter als zum Zeitpunkt der Revision grösster LE das Bundesamt für Informatik (BIT) sowie eine Rolle als Leistungsbezüger (LB) die Departemente und Verwaltungseinheiten (VE), wobei diese verschiedenen Rollen z.T. beim Generalsekretariat (GS) wieder zusammen kommen. Auf GS-Ebene will man jetzt den BR-Auftrag behandeln. Es sollen die IKT-Anforderungen definiert werden mit dem Ziel, bis ca. Mitte 2009 ein Aussprache- und Diskussionspapier zu erstellen. Mit diesem Dokument

sollten dann Umsetzungsplanungen entstehen, welche voraussichtlich wiederum zu einem Projekt führen. Derzeit ist der politische Vorprozess im Gange.

Mit den obenerwähnten Rollen muss umgegangen und die Abgrenzungen müssen klar definiert werden, auch wenn sich das EFD bezüglich einer klaren Beschreibung nicht immer schlüssig ist. So sieht sich z.B. das BIT als alleiniger LE aufgrund der eigenen Interpretation der Motion Noser. Der ISB beabsichtigte, die einzelnen Rollen eher strikt zu trennen, weil die Steuerung nicht aus der Optik eines LE erfolgen sollte, sondern LB-seitig zu führen ist. Das Verständnis der einzelnen Rollen und deren klaren Funktion ist jedoch bei allen Beteiligten noch nicht gefestigt und die Wahrnehmung obiger Rollen nicht bei allen gleich, was wiederum die Durchsetzung erschwert. Das ISB sieht sich diesbezüglich in einer Brückenfunktion für ein einheitliches Rollenverständnis.

Die EFK stellt daher fest, dass der BR-Auftrag noch nicht umgesetzt ist und pendent ist. Eine detaillierte Planung, bis wann die Umsetzung zu erfolgen hat, besteht nicht. Im Zusammenhang mit Rollen und Aufgaben haben die Prüfungen der EFK weitere, nachfolgend dargelegte Feststellungen ergeben.

Das ISB ist das Stabsorgan des IRB. Es soll helfen, Entscheide des IRB umzusetzen und zu unterstützen. Das ISB besteht aus Spezialisten in verschiedenen Fachbereichen. Die Mitarbeitenden haben zur Ausübung ihrer Aufgaben namhafte Erfahrung im betriebs-, volkswirtschaftlichen und technischen Umfeld.

Das ISB sieht die Konsenskultur als Erfolgsfaktor für den IRB als Ganzes, um bundesweite Interessen zu verfolgen und Standardisierungen, Programme und Instrumente voranzutreiben. Beschlussfassungen erfolgen durch den IRB, das ISB hat selbst wenig eigene Entscheidungskompetenz aufgrund föderaler Organisation. Es bestehen jedoch grosse Koordinationsgremien. Die Hauptaufgabe des ISB liegt darin, eine breite Konsensgrundlage zu schaffen. Ein Element davon ist die Definition und Verwendung von Standards und Normen. Standards, welche sich nicht am Geschäftsnutzen orientieren, verursachen unnötige Verwaltungskosten, deshalb braucht es vorgängig eine Priorisierung und einen klaren Willen zur Umsetzung und Einhaltung dieser Standards auf Bundesebene.

Im Weiteren ist eine der Aufgaben des ISB, Informationen und Kennzahlen in Form eines IKT-Cockpits und der Balanced Score Card (BSC) bereitzustellen. Diese Instrumente sind via IRB-Beschlüsse geregelt.

Ein verstärktes Portfolio-, Projekt-Controlling und –Reporting ist nach Auskunft des ISB u. a. auch vermehrt ein Anliegen der Finanzdelegation (FinDel). Noch nicht abschliessend geklärt ist die Frage, wie weit sich das ISB, nebst seiner unbestrittenen Verantwortung für grosse interdepartementale Programme, allenfalls auch vermehrt operativ bei Grossprojekten der einzelnen Departemente einbringen sollte. Das ISB sieht hier seine Funktion eher im Rahmen von Begleitung, Beratung, Konsolidation und Transparenzbildung. Wenn das Controlling departementaler Projekte systematisch durch das ISB durchgeführt werden sollte, dann müssten auch das spezifische Anwendungswissen und die Ressourcen ausgebaut werden. Aus Sicht des ISB muss und kann im Weiteren das IKT-Portfoliomanagement auf Stufe Bund noch verbessert werden. Ein solches könnte vermehrt Transparenz schaffen, wie die Gesamtheit der departementalen IKT-Projekte mit den übergeordneten Interessen und Vorgaben an die IKT bundesweit abgestimmt ist.

Politische Einflüsse – z.B. aus angenommenen Motionen – und das Spannungsfeld zwischen Kultur, föderalistischer Meinungsbildung und dem Versuch, auf Bundesebene zu vereinheitlichen machen es schwierig, die Standardisierung ganzheitlich durchzusetzen. Es besteht aus Sicht des ISB die Erwar-

tungshaltung, dass sich der BR mit der Führung und Steuerung der Informatik befasst. Im Bundesrat ist die IT jedoch nicht ein prioritäres Thema. Aufgrund dieses Spannungsfeldes, braucht es ständig zusätzliche Erklärungen an Parlament und BR betreffend Ressourcenbedarf mit dem Hinweis, dass sich der BR intensiver mit dem Gebiet der Informatik (IT) befassen sollte. Geschäftsverantwortliche sollten erkennen, dass die IT eine strategische Ressource ist, welche ständig an Wichtigkeit zunimmt. Da die Kernprozesse Aufgabe der Departemente und VE sind, führt dies im Hintergrund zu einer fortwährenden Diskussion zwischen den LE und LB.

Der IKT-Einsatz in der Bundesverwaltung ist auch eine Chance, das IT-Umfeld zu optimieren. Damit dies umgesetzt werden kann, wird noch eine vermehrte Transparenz benötigt, d.h. Transparenz seitens der LE BVerw-intern und -extern. Dazu braucht es ein verständliches Abrechnungs-Modell, je nachdem wie die Abrechnungen der involvierten LE als Servicecenter ausgestaltet sind.

Eine weitere Rolle im Zusammenhang mit dem Auftrag des BR besteht für das ISB darin, eine Konzentration und womöglich zentrale Steuerung der LE bezüglich der IT zu erreichen. In diesem Sinne ist auch die Motion Noser (Nr. 07.3452) zu verstehen, welche eine Konzentration der verbleibenden LE im Bereich IT beim Bundesamt für Informatik und Telekommunikation (BIT) vorsieht, mit Ausnahme jedoch von denjenigen LE, welche aus Sicherheitsüberlegungen nicht dort zentralisiert werden können.

Diesbezüglich besteht ein grundsätzliches Problem, da das VBS verstärkt daraufhin tendiert, dass IT-Anwendungen aus dem zivilen und militärischen Gebiet infrastrukturseitig zusammengelegt werden. Nach einer Realisierung ist die Umsetzung der Motion Noser erschwert oder gar praktisch verhindert.

Die Problematik eines Alleinganges des VBS und dessen Supportorgan Führungsunterstützungs-Basis (FUB) erschwert auch weitere Vereinheitlichungen und Standardisierungen, z.B. bei der Ausgestaltung der Support-Prozesse nach ITIL oder der Nutzung von gemeinsamen Know-how im Rahmen von Kompetenzzentren wie z.B. bei der Betreuung von SAP-Systemen. Diese Feststellung gilt ebenfalls für den Bereich der Public Key Infrastructure (PKI), wo das VBS eine eigene SwissDefence-PKI entwickelt hat und diese nun vertreibt. Für weitere Details verweisen wir auf Kapitel 3.6 in diesem Bericht.

Empfehlung 3.1 (Priorität 1)
Die EFK empfiehlt dem ISB, via IRB und gegebenenfalls Bundesrat eine Grundsatzentscheidung herbeizuführen, ob der Geltungsbereich der BinfV gemäss Art. 2 für das VBS aufgrund dessen IKT-Strategie geändert oder präzisiert werden muss. Insbesondere gilt es zu klären, ob die für die Einsatzsysteme der Armee vorgesehene Ausnahme auf das ganze VBS auszudehnen ist und wie in einem solchen Fall die Effizienz und Interoperabilität über die ganze Bundesverwaltung sichergestellt werden kann.

3.2 Kein wirksames Instrument vorhanden zur laufenden Überwachung und periodischen Beurteilung, ob die IKT-Strategie des Bundes erfolgreich umgesetzt wird

Die EFK hat festgestellt, dass umfangreiche Arbeiten im Rahmen der IKT-Strategie und hinsichtlich Standardisierungen durchgeführt werden. Das ISB hat sich intern entsprechend organisiert. In den

verschiedenen Fachbereichen wie Architekturen, Standards, Technologien, E-Governement, Programme, Portfolios, Controlling und Informatiksicherheit arbeiten qualifizierte Fachkräfte.

Das ISB erstellt zu Handen des IRB Entscheidungsgrundlagen wie den Sicherheitsbericht oder die Balanced Score Card (BSC). Zudem verfügt es über das IKT-Cockpit. Hinsichtlich dem IKT-Cockpit können die Departemente und die Bundeskanzlei ihre IKT-Objekte (Studien, Projekte und Anwendungen) entweder direkt erfassen oder mit eigenen Werkzeugen arbeiten und ihre Objekte über eine Schnittstelle ins IKT-Cockpit übermitteln. Es wäre eine Vorgabe, dass auf diese Art und Weise alle IKT-Objekte der Departemente und der Bundeskanzlei im IKT-Cockpit laufend eingepflegt werden und auf dem ISB zugänglich sind. Auf Stufe Bund ist das IKT-Cockpit vor allem als Werkzeug für das Portfoliomanagement gedacht. Auf Stufe Departement und Amt kann das IKT-Cockpit sowohl als Werkzeug für das Einzelprojektcontrolling wie auch als Portfoliomanagement eingesetzt werden. Es bestehen jedoch noch Lücken bei der Vollständigkeit der IKT-Cockpit-Daten. Das ISB schätzt, dass zurzeit etwa 70% alle IKT-Objekte der BVerw auf Stufe Bund im IKT-Cockpit ersichtlich sind. Die Datenbasis des IKT-Cockpits wird anhand einer Selbstdeklaration der Departemente nachgeführt, was zu unvollständigen Zahlen führt wenn eine bestimmte OE dieser Aufgabe nicht vollumfänglich nachkommt. Alleine mit der Integration der Zahlenbasis seitens des VBS würde eine Erhöhung der Vollständigkeit um approximativ 20% erreicht.

Eine Überprüfung der EFK ergab zudem, dass zum Zeitpunkt der vorliegenden Berichtserstellung nur knapp 60% der IKT-Wachstumsgelder im IKT-Cockpit erklärbar und abgebildet waren. Zu den restlichen 40% fehlen die entsprechenden Informationen seitens der Organisationseinheiten (OE).

Empfehlung 3.2.1 (Priorität 1)
Die EFK empfiehlt dem ISB via IRB zu erwirken, alle Studien, Projekte und Anwendungen aller Departemente und der Bundeskanzlei auf Stufe Bund im IKT-Cockpit zu integrieren.

Das ISB hat die erwähnte BSC entwickelt, um u.a. pro Departement verschiedene IT-Kostenfaktoren zu erheben und vergleichen zu können. Es werden auch bundesweit übergeordnete Zahlen – z.B. Anteil IKT-Kosten am gesamten Funktionsaufwand des Bundes – erhoben. Diese BSC wird jährlich erstellt und enthält interessante, aber auch erklärungsbedürftige Zahlen und Vergleiche. Das Ziel der BSC ist u.a., Führungskennzahlen und Kostenvergleiche im IT-Bereich darzulegen.

Die BSC wurde zum vierten Mal erstellt. Die aktuellste Version per 8. Dezember 2008 ist dem IRB im Februar 2009 präsentiert worden. Die Mehrjahresvergleichbarkeit ist noch schwierig, da die Berechnungsbasis für diverse Kenngrössen in diesen vier Jahren auf Wunsch des IRB verändert wurden und damit Zeitreihenanalysen nur bedingt aussagekräftig sind. Z. B. wird die Kenngrösse «LB seitige Kosten» im IRB immer wieder diskutiert. Verschiedene Parameter beeinflussen die Ergebnisse, wie anhand der Arbeitsplatzkosten dargelegt werden kann: Einige Departemente haben häufig LE-Unterstützung nötig währendem andere eigenes Personal für den 1st-Level Support einsetzen. Je nachdem erscheinen diese Aufwendungen dann nicht in der Kennzahl «Anzahl IKT LB Vollzeitstellen». Im Weiteren gibt es Departemente, bei welchen höhere Kosten aufgrund der grösseren Anzahl Fachanwendungen entstehen, was zu einer hohen Varianz bei den Werten der verschiedenen Departemente führt. Zusätzlich ist eine gewisse Ungenauigkeit bei solchen Zahlenerhebungen häufig vorhanden.

Ein weiterer Grund für eine Ungenauigkeiten liegt in der mangelnden Bereitschaft seitens der LE, präzise und verständliche Zahlen zu liefern, da Vergleiche mit anderen LE nicht durchgehend erwünscht sind wie z.B. beim Vergleich der Netzwerkkosten oder der LE-seitigen Arbeitsplatzkosten.

Nach Einschätzung des ISB wird der BSC im IRB noch zu wenig Beachtung zugemessen, wobei jedoch aus Sicht der EFK diese Vergleichszahlen eine interessante Grundlage bilden, um Kostenunterschiede zu vergleichen, weitere Verbesserungen zu erzielen und ggf. strategische Entscheidungen zu begründen. Auch wenn verschiedene Zahlen z.T. ungenau sind, können sie Hinweise auf langfristige Entwicklungen geben. Daher macht ein Mehrjahresvergleich mit möglichst unveränderten Berechnungsparametern Sinn. Die Vollständigkeit der Datenlieferungen sollte soweit als möglich angestrebt werden.

Empfehlung 3.2.2 (Priorität 1)
Die EFK empfiehlt dem ISB, via IRB möglichst vollständige und genaue Datenlieferungen seitens der Leistungserbringer (LE) und betroffenen Departemente hinsichtlich IT-Kosten zu erwirken und diese in die Balanced Score Card (BSC) einfliessen zu lassen.

Das ISB ist für die IKT-Strategie (aktuellste Fassung vgl. ISB 2007-11) des Bundes zuständig. Diese wird im Intranet publiziert, wie auch alle Standardisierungen und Dokumente zu diesem Thema (siehe auch intranet.isb.admin.ch; andere z.B. www.egovernment.ch) und weitere wichtige Grundlagen wie die IRB-Beschlüsse (siehe unter www.irb.admin.ch).

Durch die Berichterstattungen an den IRB und die Departemente ist das ISB auch als „Temperaturfühler“ prädestiniert um zu beurteilen, ob die IT-Strategie des Bundes noch stimmt oder überarbeitet werden sollte. Richtungsänderungen hinsichtlich der Strategie werden häufig aus der Politik ausgelöst (z.B. Motion Noser Nr. 07.3452, Motion Finanzkommission NR 05.3470, usw.). Für Parlamentarier sowie auf Ebene der Amtsleitungen sind Führungskennzahlen ein Indikator, um strategische Entscheidungen transparent zu machen. Solche Hinweise werden u.a. mittels der periodischen BSC (mit ca. 30 Kennzahlen, wie z.B. Kosten pro PC-Arbeitsplatz) erstellt und an den IRB kommuniziert. Weitere Personenkreise sind nicht automatisch Empfänger dieser BSC.

Aufgrund der Wichtigkeit und Aussagefähigkeit dieser BSC erachtet es die EFK als sinnvoll, möglichst alle relevanten Ansprechpartner über Führungskennzahlen zu informieren.

Empfehlung 3.2.3 (Priorität 2)
Die EFK empfiehlt dem ISB, die erlangten Informationen und bekannten Kostenvergleiche auf Ebene Parlamentarier, Departements- und Amtsleitungen periodisch und aktiv zu präsentieren.

Das ISB als Stabstelle des IRB schlägt die IT-Strategie des Bundes vor, welche der IRB anschliessend offiziell genehmigt. Viele Elemente der Strategie sind durch die Departemente umzusetzen. Für die Durchsetzung und Kontrolle der Einhaltung der IT-Strategie besitzt das ISB jedoch keine offizielle Funktion, um die Einhaltung der IT-Strategie zu überwachen, da dies gemäss BinfV dem IRB zugewiesen ist. Nach Diskussion mit dem ISB ist unklar, wer die Überwachungsfunktion in der Praxis durchführt, da bisher keine entsprechenden Aufträge erteilt wurden. Eine offizielle Möglichkeit, die Durchsetzbarkeit der IT-Strategie zu forcieren, fehlt dem ISB.

Aus Sicht der EFK ist eine Überwachung über die Einhaltung der IT-Strategie eine wichtige Aufgabe, welche durchzuführen ist. Diese sollte im Rahmen einer operativen Kontrollfunktion vom IRB bestimmt und durchgeführt werden.

Empfehlung 3.2.4 (Priorität 1)
Die EFK empfiehlt dem ISB via IRB, die Aufgaben des IRB (gemäss BinfV Art. 13, Abs. 2 Buchstabe a) betreffend der Überwachungsfunktion wo nötig zu präzisieren und konsequenter umzusetzen, was die Einhaltung der Informatikvorgaben betrifft.

Diese Überwachungsfunktion sollte gleichzeitig die Kontrolle über die Einhaltung von definierten Normen und Standards im IT-Bereich beinhalten (siehe Kapitel 3.3).

3.3 Das ISB bzw. die Bundesverwaltung verfügt nicht über die notwendigen Instrumente und Strukturen, um festgelegte Normen und Standards durchzusetzen

Das ISB entwickelt Normen und Standards, welche für die IT innerhalb der BVerw gelten. Die Publikation erfolgt über das Intranet, je nach Bereich auf verschiedenen Intranet-Adressen (z.B. auf dem Gebiet des E-Governement auf www.ech.ch, für die weiteren Standards auf www.isb.admin.ch).

Die bestehenden Bundesstandards werden soweit gut gepflegt, wie die Handlungsfähigkeit und Kompetenz es dem ISB erlauben. So werden diese Standards einerseits aktiv bzw. auf Anfrage in den verschiedenen Organisationseinheiten präsentiert. In Schulungen mit entsprechenden Themen wird ebenfalls darauf hingewiesen. Die Standards werden in grossen, vom ISB geleiteten Programmen aktiv angewendet. Daraus ergeben sich Erkenntnisse, welche es dem ISB erlauben, die bestehenden Standards und Normen auf einem praxisgerechten, aktuellen Stand zu halten und ständig zu verbessern bzw. wo notwendig zu vereinfachen.

Im Weiteren beobachtet das ISB internationale Standardisierungsbestrebungen, um neue Trends vorzeitig zu erkennen und ggf. in die Bundesstandards einfliessen lassen zu können. Das ISB ist ebenfalls mit der E-Governement-Gruppe in zusätzlichen Technologie-Gremien in Verbindung. Aktuelles Beispiel dazu ist das Entwicklungsvorgehen mittels Service Oriented Architecture (SOA). Ein aktuelles Beispiel dazu sind die IKT-Prozesse im Bereich IKT-Betrieb und -Support [siehe Prozesse P06 und P07 in **Beilage 3**]. Dort hatte der IRB schon früh ein eigenes Modell entwickelt, weil sich noch kein Standard international durchsetzen konnte. In den vergangenen Jahren etablierte sich auf dem Gebiet des IT-Services Management die Information Technology Infrastructure Library (ITIL). Das ISB hat den eigenen Standard daraufhin überarbeitet bzw. vereinfacht. Dabei wurden unter anderem auch die neuen Versionen von ITIL berücksichtigt. Die Verbindlichkeit der bundesspezifischen IKT-Prozesse P06 und P07 [siehe **Beilage 3**] soll zu Gunsten von ITIL V3 zurückgestuft werden.

Eine weitere allgemein bekannte Standardisierung für das Projektmanagement [siehe Prozess P05: Lösungen entwickeln in **Beilage 3**] ist HERMES, welche von der Bundesverwaltung in den frühen 90er-Jahren festgelegt wurde. HERMES hat sich unterdessen zu einem anerkannten Grundsatz etabliert. Im Bereich der Projektleitung kann auch ein anerkanntes Zertifikat erworben werden. Das Ziel ist, in grossen Projekten und Programmen nur noch zertifizierte Projektleiter einzusetzen, um die effiziente Umsetzung zu erhöhen.

Als Stabsorgan des IRB kann das ISB aus seinen Tätigkeiten entsprechendes Know-how gewinnen und Entwicklungen im Rahmen von Normen und Standards optimal vorschlagen. Das ISB ist ebenso in den verschiedenen Fachgruppen wie dem A-IS, dem ABB, dem FBB und dem PAB vertreten oder hat einzelne Gruppen gegründet. So steht ebenfalls praxisorientiertes Know-how für Standardisierungsarbeiten zur Verfügung, um diese an den strategischen Vorgaben des Bundes auszurichten.

Die Umsetzung dieser Normen und Standards liegt vorwiegend bei den entsprechenden Departementen und VE, welche IT-Projekte führen bzw. grössere Ablösungen von bestehenden Anwendungen planen. Für die Gewinnung der Kenntnisse von anzuwendenden Normen und Standards handelt es sich primär um eine Holschuld der Projektleitenden. Ein systematischer Informationsaustausch über einzuhaltende Normen und Standards zwischen dem ISB und den Projektführenden findet nicht statt. Eine Aufsicht oder sogar eine Überwachungsfunktion mit Möglichkeiten zum Intervenieren bei Nichteinhaltung besitzt das ISB nicht. Das ISB ist teilweise über die verwendeten Standards durch den Einsitz in den IT-Programmen und -Projekten oder das Beziehungsnetz informiert, ohne dass dies jedoch vollumfänglich und zwangsläufig, sondern nur vereinzelt sichergestellt ist.

Die EFK erachtet es als wichtig, dass generell und vollständig über die Berücksichtigung und Einhaltung von Standards und Normen in den aktiven und zu berücksichtigenden IT-Projekten sowie IT-Programmen systematisch informiert wird.

Empfehlung 3.3.1 (Priorität 2)
Die EFK empfiehlt dem ISB, in allen grösseren bzw. technologisch wichtigen IT-Projekten und –Programmen Einsitz zu erhalten und dabei auf die Berücksichtigung und Einhaltung von Standards und Normen systematisch hinzuwirken.

Eine spezifische Weisung, welche die Überwachung über die praxisbezogene Durchsetzung von Normen und Standards durch das ISB oder eine anderweitige Organisation regelt, besteht nicht, obwohl der IRB für die Überwachung der Informatikvorgaben verantwortlich ist.

Aus Sicht der EFK ist eine Überwachungs- und Kontrollfunktion über die Einhaltung von Normen und Standards im IT-Bereich ein notwendiges Instrument, damit diese Normen und Standards auch operativ durchgesetzt werden. Diesbezüglich verweisen wir auf die vorstehende Empfehlung 3.2.4.

Zu oben erwähnter verbesserungsfähigen Durchsetzung gehört auch, dass keine generelle strategische Informatikplanung (SIP) auf Bundesebene besteht, welche die Leitplanken und längerfristigen Planungen auf dem Gebiet der IT beinhaltet, wie dies gemäss BinfV vorgesehen ist (Art. 3, Abs 1.a und 2). Auf Stufe Departement und verschiedener VE besteht teilweise eine SIP, welche jedoch zu Interessen- und Abstimmungskonflikten mit definierten Standards und Normen führen kann, sofern diese nicht mit einer bundesweit geltenden SIP abgestimmt wird.

Die EFK erachtet eine SIP auf Stufe Bund für wichtig, damit den definierten Normen und Standards eine längerfristige Grundlage zur Seite gestellt werden kann. Diese SIP sollte mit jenen der Departemente abgestimmt sein.

Empfehlung 3.3.2 (Priorität 2)
Die EFK empfiehlt dem ISB, auf Bundesebene eine strategische Informatikplanung als geltende Grundlage der IKT-Strategie und zur Durchsetzung von Normen und Standards im IT-Bereich zu erstellen.

3.4 Die Einhaltung von Normen und Standards scheint subjektiv beurteilt verbesserungsfähig

Das ISB hat eine so genannte Prozesslandkarte entwickelt, an der sich das Vorgehen hinsichtlich Informatik bei den Departementen und VE orientieren sollte. Anhand dieser Prozesse werden auch die gültigen Normen und Standards definiert und in Kraft gesetzt. Dies erfolgt im Rahmen des Prozesses P01 (Informatik steuern).

Die vollständige Prozesslandkarte mit Aktivitätenangaben und Rollen ist in **Beilage 3** ersichtlich.

Die Prozessdefinitionen sind kompatibel bzw. werden zurzeit erneut mit internationalen Standards wie z.B. ITIL abgestimmt, welcher das IT Service Management vereinheitlicht und standardisiert.

Die Verbreitung und Kommunikation der Prozessvorgaben in den OE erfolgen grundsätzlich über den IRB und die diesbezüglichen Vertreter der Departemente. Die Fachleute aus dem ISB haben teilweise Einsitz in den Ausbildungen oder in Projekten. Die Fachgruppe „Zusammenspiel und Verbindlichkeit der IKT-Prozessvorgaben“ (ZV-IPV) hat den Auftrag, ITIL und andere Standards und Normen gegenüber den Prozessen neu zu positionieren.

Die Einhaltung der Prozesse, Definitionen sowie Normen und Standards liegt bei den Departementen. Inwieweit die Prozessvorgaben durchgesetzt werden bzw. welche Wirkung die Prozesse erzielen, kann aus Sicht des ISB nur bedingt beurteilt werden, da ein Prozess-Assessment (Bewertung der Prozessumsetzung) oder eine Prozess-Messung (Bewertung der Prozesswirkung) nicht erfolgt. Dies wäre zwar methodisch möglich, wurde bisher jedoch aus Ressourcengründen nicht durchgeführt. Zudem ist die direkte Zuständigkeit des ISB auf die Stufe Bund beschränkt.

Eine gängige Beurteilungsmethode basiert auf dem Capability Maturity Model Integrated (CMMI), welches den Reifegrad eines Prozesses beurteilt. Dabei wird eine Bewertung von 0-5 nach folgendem Schema vergeben:

Maturity Model nach COBIT 4.1
(Control Objectives for Information and related Technology)

- 0 = non existent (nicht existent)
- 1 = initial / ad-hoc (initial)
- 2 = repeatable but intuitive (wiederholbar aber intuitiv)
- 3 = defined (definiert)
- 4 = managed and measurable (geführt und messbar)
- 5 = optimised (optimiert)

[3] *IRB-Beschluss 2006-069-230, Trakt. 2.3 vom 2006-02-27*

Nach Einschätzung des ISB ist die Umsetzung der standardisierten Prozesse bisher sehr unterschiedlich eingehalten worden, der Reifegrad nach COBIT wird jedoch über alles betrachtet höchstens mit der Stufe 1 (Initial) beurteilt. Genauere Informationen und Angaben diesbezüglich sind aufgrund fehlender Assessments nicht verfügbar. Eine Umfrage des ISB wurde im März 2009 an die Departemente versandt mit dem Ziel, Rückmeldungen über die Anwendung von Standards und Praktiken im Bereich der IKT-Prozesse zu erhalten. Die Rücklaufquote war ungenügend, so dass keine repräsentative Aussage möglich ist.

Die Einhaltung von Normen und Standards wird beim ISB aufgrund der Prozessdurchsetzung nur grob geschätzt, es zeigen sich jedoch Unterschiede bei der Beurteilung pro Prozess. Generell sollte ein Zielwert von 2 gemäss COBIT aus Sicht des ISB erreichbar sein.

Die Prozesse und die Definition von Standards und Normen sind Bestandteile der gesamten IKT-Strategie des Bundes. Es ist jedoch aufgrund obenerwähnter Darlegung derzeit nicht möglich, eine genaue Aussage über die Einhaltung dieser Bundesstandards zu formulieren. Ebenso wenig kann die Beurteilung abschliessend erfolgen, ob im Sinne der IKT-Strategie des Bundes gehandelt wird.

Die EFK erachtet eine periodische Beurteilung und Messung der Einhaltung von Prozessen und Standards als wichtig, damit das ISB und die VE eine Standortbestimmung vornehmen können.

Empfehlung 3.4 (Priorität 2)
Die EFK empfiehlt dem ISB, mit einer detaillierten Erhebung die Einhaltung von Informatikvorgaben gem. BinfV jährlich zu ermitteln. Je nach Ergebnis sind Massnahmen zur Umsetzung der Einhaltung zu definieren.

3.5 Synergiepotenziale werden noch nicht optimal genutzt und Doppelspurigkeiten sind vorhanden

Ein mögliches Gebiet, um finanzielle und technologische Synergien in der IT zu erwirken, besteht in der Ausnutzung von Skaleneffekten, indem Erhöhungen in der Anzahl von betreuten Applikationen und Netzwerkbelastungen nicht unbedingt zu einer linearen Kostenerhöhung führen. Dies ist auch der Hintergrund der Motion Noser (Nr. 07.3452) wie bereits in Kapitel 3.1 erwähnt.

Aus heutiger Sicht ist die Umsetzung dieser Motion noch weit entfernt, da verschiedene LE für sieben Departemente IT-Leistungen erbringen. Hinzu kommen die Bestrebungen seitens des VBS, seine Applikationen, unabhängig davon ob diese im militärischen oder zivilen Bereich genutzt werden, in eine einzige IT-Umgebung zu bündeln, was die vollständige Umsetzung der erwähnten Motion im VBS behindert.

In diesem Zusammenhang verweisen wir ebenfalls auf die vorstehende Empfehlung 3.1 und die Ausführungen im Kapitel 3.6 des vorliegenden Prüfberichts.

Auch unabhängig von der Entwicklung im VBS bestehen technologische Synergiepotenziale, da weiterhin verschiedene LE IT-Dienstleistungen auf ähnlichen Gebieten erbringen. So befassen sich mehrere LE mit neuen Technologien wie Service Oriented Architecture (SOA), welche bei verschiedenen Projekten und Programmen zur Anwendung gelangen. Dies führt jedoch zu einem Ausbildungsbedarf bei verschiedenen Stellen und Organisationen. Zudem wird die Einheitlichkeit der Umsetzung erschwert, was später erhöhte Wartungskosten ergeben kann. Ähnliche Gegebenheiten bestehen in

verschiedenen Bereichen und Departementen für eingesetzte Standardanwendungen wie z.B. SAP, wo zwei Kompetenzzentren (CC-SAP des BIT und CC-SAP der FUB) bestehen.

Aus Sicht der EFK besteht noch ein beträchtliches Einsparungspotenzial, sofern eine weitere Konzentration auf möglichst wenige LE aufgrund der Skaleneffekte zu marktgerechten Preisen durchsetzbar ist. Dies bedingt einerseits eine Organisationsform des LE, welcher sich an internationalen Standards wie z.B. ITIL orientiert und andererseits eine Kostenkontrolle durch die LB, um die offerierten Leistungen transparent vergleichen zu können. Das bedeutet auch, dass ein LE benchmark-fähig sein muss, damit die Leistungen klar abgrenzbar und transparent darstellbar sind, Dies könnte durch eine standardisierte Ausgestaltung der SLA erreicht bzw. unterstützt werden.

Empfehlung 3.5.1 (Priorität 1)
Die EFK empfiehlt dem ISB, einen Umsetzungsplan für die Motion Noser (Nr. 07.3452) mit dem Ziel zu erstellen, eine Konzentration auf möglichst wenige oder nur noch einen Leistungserbringer zu erreichen und dabei die Grundsatzentscheidung, wie weit das VBS dem Geltungsbereich der BinfV zukünftig noch unterliegt (siehe Empfehlung 3.1), zu berücksichtigen.

Empfehlung 3.5.2 (Priorität 1)
Die EFK empfiehlt dem ISB, eine SLA-Standardisierung für Betrieb und Unterhalt von IT-Anwendungen und der Büroautomation anzustreben, mittels derer ein Leistungserbringer vergleichbare und transparent dargelegte Kosten offerieren muss. Dabei ist auch auf die Einhaltung internationaler Standards – wie z.B. ITIL, Einhaltung der IT-Sicherheitsorganisation gemäss ISO 27001, usw. – zu achten. Dies gilt vor allem für sogenannte Commodities, d.h. für bundesweit verwendete Standarddienste und –produkte bzw. Services im Bereich der IT.

3.6 Die Notwendigkeit einer SwissDefence-Public Key Infrastructure des VBS ist noch nicht abschliessend dargelegt

Ziel der Revision der EFK von April bis Juli 2009 im Informatikstrategieorgan des Bundes (ISB) ist die Beurteilung, ob die Informatikstrategie in der Bundesverwaltung wirksam und im Sinne der strategischen Vorgaben umgesetzt wird. Zu diesen Vorgaben gehören auch die vom Informatikrat Bund (IRB) festgelegten Querschnitts-Dienstleistungen (Q-DL) und der damit verbundene Bezugszwang. Die vom Bundesamt für Informatik und Telekommunikation (BIT) betriebene Public Key Infrastructure (AdminPKI) wurde 2004 durch den IRB in den Katalog der Q-DL aufgenommen. Das Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) hat in den letzten Wochen Anträge an den IRB eingegeben, um die eigene SwissDefence PKI (SD-PKI) bewilligen zu lassen. Aus aktuellem Anlass behandelt die EFK die Q-DL AdminPKI in einem vorgezogen Teilbericht (siehe **Beilage 5**).

Die AdminPKI des BIT
Die Grundsätze für eine PKI-Bund (AdminPKI) legte der IRB im Jahre 2003 fest und entschied, dass eine einzige PKI in der Bundesverwaltung verwendet werden und das BIT diese Leistung erbringen soll. Der IRB nahm in der Folge die AdminPKI in den Katalog der Q-DL auf und finanzierte diese auch teilweise mit Querschnitts-Geldern des Bundes. Die vom BIT aufgebaute AdminPKI umfasst die Ausgabe von Zertifikaten der Klassen A bis D. Das BIT als Anbieter der in der ZertES (Gesetz über die elektronische Unterschrift) definierten Zertifikate wurde im Jahre 2007 durch die KPMG zertifiziert.

Dazu musste es sehr hohe Qualitäts- und Sicherheitsanforderungen erfüllen. Bisher wurden durch die AdminPKI 52‘200 Zertifikate ausgegeben, davon 37‘000 der Klasse B. Die Benutzenden der Smart-Card mit der Klasse B sind zu 80% in den Kantonen und zu 20% in der Bundesverwaltung angesiedelt. Die Kosten für Aufbau und Betrieb einer PKI sind hoch. Das BIT hat bisher einen Kostendeckungsgrad von 65% erreicht. Damit eine Vollkostendeckung erreicht wird, müssten 100‘000 Zertifikate ausgestellt werden können.

Die SwissDefence PKI des VBS

Das VBS plante aus militärischen Sicherheitsüberlegungen eine eigene PKI aufzubauen und startete daher im Jahre 2005 ein Projekt zur Entwicklung eines Testsystems SD-PKI. Es entstand in der Folge das „Militärische Pflichtenheft zur Entwicklung und zum Ausbau der permanenten Basisleistungen der SwissDefence PKI“. Dieses stellt den Projektauftrag für den Rollout der Smart-Cards dar. Das Testsystem der SD-PKI ist seit 2006 operativ. Auf diesem System wurden bisher rund 300 Smart-Cards zu Test- bzw. Pilotzwecken generiert, diese sind noch nicht produktiv im Einsatz. Nun ist der rasche Rollout der 15‘000 Zertifikate (äquivalent zu Klasse B der AdminPKI) ab Juni 2009 vorgesehen.

Abklärungen und Entscheide sind zu treffen

Ein Antrag zur Anerkennung der SD-PKI wurde dem IRB seitens des VBS im April 2009 gestellt. Der IRB hat diesen zurückgestellt und wartet ab, bis eine Sitzung auf Stufe Generalsekretariat VBS und Eidg. Finanzdepartement Klärung bringt, wie zukünftig mit dem strategischen Vorhaben „Zusammenführung von Armee- und Verwaltungsinformatik im VBS“ umzugehen ist. Ausnahmebewilligungen für zentrale Dienstleistungen schaffen Präjudiz und untergraben in der Regel den wirtschaftlichen Einsatz von Finanzmitteln. Ein strategischer Entscheid drängt sich auf, da verschiedene Zeichen auf eine Abspaltung des VBS von der übrigen Bundesverwaltung hindeuten. Dieser Trend wurde auch sichtbar bei SAP, beim „Forest Bund“ und der Kündigung der Service Level Agreements „Netzdienstleistungen“. Es bleibt somit zu klären, wie weit das VBS künftig zur Bundesverwaltung gehört und damit die Vorgaben einzuhalten hat. Bei diesem Entscheid sollten neben den militärischen Aspekten auch das Kosten-/Nutzenverhältnis und die Mehrkosten berücksichtigt werden.

Damit die Gründe für die Schaffung einer VBS-eigenen PKI besser verstanden werden können und eine optimale Investitionssicherung gefunden werden kann, **empfiehlt die EFK dem VBS**

- dem BIT die konkreten VBS-Anforderungen an die Zertifikate und die AdminPKI darzulegen und die Möglichkeiten abzuklären, welche zur Erfüllung dieser Anforderungen führen können (Empfehlung 8.1 in **Beilage 5**);
- dem IRB darzulegen, welche Systeme und/oder Anwendungen sich im militärischen Bereich (Waffensysteme oder FUB) zum heutigen Zeitpunkt der SD-PKI bedienen (Empfehlung 8.2 in **Beilage 5**);
- dem IRB, die dargestellten Kosteneinsparungen und Effizienzsteigerungen durch nachvollziehbare Berechnungen zu belegen (Empfehlung 8.3 in **Beilage 5**).

Die **EFK empfiehlt dem IRB**, dass Ausnahmebewilligungen oder Sonderregelungen, die eine Querschnittsdienstleistung betreffen oder aufgrund anderweitiger Regelungen einen Bezugszwang tangieren, ohne zwingende Gründe nicht bewilligt werden. Falls nicht anders möglich, sollten strategische Entscheide auf Stufe Bundesrat gesucht werden (Empfehlung 8.4 in **Beilage 5**).

Der IRB hat den erwähnten Teilbericht der EFK (siehe **Beilage 5**) zur Kenntnis genommen und anlässlich der Sitzung vom 25. Mai 2009 folgendes protokollarisch festgehalten (Beschluss-Nummer 2009-102-220):

1. [redacted]
2. [redacted]
3. [redacted]
4. [redacted]
5. [redacted]
6. [redacted]

Die Verantwortlichen des VBS haben zu den Feststellungen und Empfehlungen eine andere Sichtweise und sind in wesentlichen Teilen damit nicht einverstanden. Die kontrovers geführten Diskussionen betreffend PKI zwischen VBS und IRB bzw. ISB oder dem BIT werden aus Sicht des VBS behindert, weil vorgängig generelle Entscheidungen auf Stufe Bund über die Steuerung und Führung der IT zu treffen wären.

Entsprechend der Entscheidungen des IRB und Reaktionen des VBS sind gewisse Empfehlungen teilweise erledigt bzw. bereits überholt (Empfehlungen 8.2 und 8.4 in **Beilage 5**).

3.7 Der Status von Empfehlungen bzw. die Umsetzung vorgesehener Massnahmen aus früheren Revisionen zeigt, dass Pendenzen bestehen

Infolge anderer Prioritätensetzung der EFK konnte kein umfassender Follow-up für die im Zuge der früheren Prüfungen (5037_Budgetprozess IT Invest EFD, 5039_Org & Aktivität ISB, 7296_QP KNW bei IKT-Grossprojekten und 7402_SAP-Strategie) abgegebenen Empfehlungen und vorgesehenen Massnahmen erfolgen.

Es wurde jedoch der Status der einzelnen Empfehlungen aus Sicht des ISB erhoben, welcher ergab, dass für die Umsetzung der Empfehlungen noch Pendenzen bestehen und die Resultate bzw. Vorgaben aus der laufenden Überprüfung "Steuerung und Führung des Einsatzes der Informations- und Kommunikationstechnologie in der Bundesverwaltung" abgewartet werden, welche der BR in Auftrag gegeben hat. Ebenso könnte allenfalls die nun anlaufende Zentralisierung der IKT-Leistungserbringer (Motion Noser Nr. 07.3452) im Rahmen der Aufgabenüberprüfung des Bundes Einfluss auf die Steuerungs- und Führungsmethoden und -werkzeuge der IKT und daher die Empfehlungen haben.

Zudem ist zu beachten, dass im Auftrag des IRB zur Zeit (siehe Beschlüsse des IRB vom Juni 2009) im Rahmen des Kontinuierlichen Prozess-Managements (KPM) Arbeiten laufen mit dem Ziel, das IKT-Prozesssystem zu vereinfachen und zu straffen, die Hierarchie der IKT-Vorgaben zu konsolidieren und bestehende Standards wie ITIL, COBIT oder TOGAF zu berücksichtigen sowie darauf aufbauend auch das IKT-Governance-System zu verbessern.

Im Weiteren betrafen einige Empfehlungen nicht direkt das ISB. Die vollständige Liste mit dem Status aller Empfehlungen und Umsetzung vorgeschlagener Massnahmen ist aus unseren Arbeitspapieren ersichtlich.

4 Schlussbesprechung

Das Ergebnis der Prüfung wurde am 31. August 2009 besprochen. Von unseren Ausführungen und Hinweisen wurde Kenntnis genommen.

Allen Mitarbeitenden des ISB sei für die gewährte Unterstützung bestens gedankt.

EIDGENÖSSISCHE FINANZKONTROLLE

Massimo Magnini	Hans-Jörg Uwer
Fachbereichsleiter	Revisionsleiter

Beilagen

Beilage 1 – IT-Governance
Beilage 2 – Organisation des ISB
Beilage 3 – Prozesslandkarte
Beilage 4 – Empfehlungsübersicht
Beilage 5 – Detailbericht SD-PKI