PRÜFBERICHT

EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Prüfung der Sicherheit und des Vertragswesens im Informatikbereich

Parlamentsdienste

03. November 2014

EFK 14238 – mit integrierter Stellungnahme der Parlamentsdienste – zur Veröffentlichung

Das Wesentliche in Kürze

Im Rahmen des Prüfprogramms 2014 hat die EFK bei den Parlamentsdiensten (PD) den Informatik- und Beschaffungsbereich geprüft. Es standen vor allem die Auslagerung der Informatik, die Auftragsvergaben und die Informatiksicherheit im Vordergrund. Bei den Vergaben wurden elf, teilweise mehrjährige Geschäfte von insgesamt rund 4 Mio. Franken kontrolliert. Das jährliche Finanzvolumen beträgt rund 8,8 Mio. Franken.

Die Auslagerung der Informatik erfolgte auf Basis eines Variantenvergleichs zwischen externer Lösung, dem BIT als Dienstleistungslieferanten und einer PD-internen Lösung und wurde von der Verwaltungsdelegation der eidgenössischen Räte genehmigt. Nach wie vor ist die gewählte externe Lösung im Vergleich zu den ursprünglichen Kosten die wirtschaftlich günstigste der drei Varianten ist. Dies auch bei inzwischen höheren Betriebs- und Unterhaltskosten aufgrund gestiegener Anforderungen.

Die Prüfung der Informatiksicherheit zeigt, dass diverse Massnahmen ein angemessenes Schutzniveau bieten. Wesentliche Risiken sind jedoch sowohl bei den Parlamentsdiensten als auch bei den Parlamentariern abhängig vom persönlichen Verhalten der Benutzer. Deshalb ruft der Dienst für Informatik und neue Technologien seinen internen Mitarbeitenden wichtige Regeln im Umgang mit elektronischen Geräten und Daten immer wieder in Erinnerung.

Einige Empfehlungen aus 2011 sind noch nicht zufriedenstellend umgesetzt. Dies betrifft die beschaffungsspezifischen Vorgaben, den Ablauf sowie die Dokumentation eines IKS für den Beschaffungsbereich. Die PD wollen nun das bisher auf Human Resources und Finanzen beschränkte IKS auch auf die Risiken im Beschaffungsbereich ausdehnen.

Die PD sind mit den Empfehlungen der EFK einverstanden und wollen alle Empfehlungen bis Ende 2015 umsetzen.

L'essentiel en bref

Dans le cadre du programme d'audit de 2014, le Contrôle fédéral des finances (CDF) a examiné l'informatique et les acquisitions des Services du Parlement (SP). L'audit portait principalement sur l'externalisation des services informatiques, l'attribution des mandats et la sécurité informatique. Le CDF s'est penché sur onze adjudications qui portent, pour certaines d'entre elles, sur des affaires s'étendant sur plusieurs années, et qui représentent un montant total d'environ 4 millions de francs. Le volume financier annuel, quant à lui, se monte à près de 8,8 millions de francs.

L'externalisation des services informatiques a été décidée après avoir analysé trois options : solution externe, recours à l'Office fédéral de l'informatique et de la télécommunication en tant que fournisseur de prestations ou solution interne aux SP. La Délégation administrative des Chambres fédérales a approuvée le choix de la solution externe. En comparaison avec les coûts initiaux, cette solution demeure la plus économique des trois, et ce malgré une hausse, survenue entre-temps, des coûts d'exploitation et d'entretien découlant de l'augmentation des exigences.

Les SP ont pris diverses mesures pour garantir un niveau de protection approprié de sécurité informatique. Certains risques majeurs dépendent du comportement individuel des utilisateurs, aussi bien au niveau des SP qu'au niveau des parlementaires. Pour cette raison, le service Informatique et technologies nouvelles rappelle régulièrement aux collaborateurs les règles importantes à observer lors de l'utilisation d'appareils électroniques et du traitement de données.

Quelques recommandations datant de 2011 n'ont pas encore été appliquées de manière satisfaisante. Il s'agit en particulier des directives en matière d'acquisitions ainsi que du processus et de la documentation d'un système de contrôle interne dans ce même domaine. Les SP souhaitent à présent élargir le système de contrôle interne, qui ne s'applique pour l'instant qu'aux ressources humaines et aux finances, aux risques liés aux achats.

Les SP approuvent les recommandations du CDF et prévoient de toutes les appliquer d'ici à fin 2015.

Generelle Stellungnahme der Parlamentsdienste (PD):

Wir bestätigen den Eingang Ihres Berichtsentwurfs und bedanken uns dafür. Mit Befriedigung nehmen wir zur Kenntnis, dass die beiden Prüfbereiche „Auslagerung der Informatik" sowie „Informatiksicherheit" zu keinen materiellen Feststellungen führten.

Aus unserer Sicht bestätigt der Bericht, dass die Parlamentsdienste im Bereich der Beschaffung auf dem richtigen Weg sind und seit der letzten Prüfung 2011 Fortschritte erzielt haben. Dass dieser Teil allerdings noch Mängel aufweist ist nicht überraschend. Wir bestätigen, dass die Feststellungen im Bericht der EFK nachvollziehbar, verständlich und hilfreich sind. Die Details unserer Umsetzungsmassnahmen finden Sie in der Empfehlungsübersicht in der Beilage.

Der guten Form halber bestätigen wir Ihnen ebenfalls, dass wir Ihre Feststellung zur einzigen noch nicht vollständig umgesetzten Empfehlung aus der Prüfung 11324 (Empfehlung 3.3) zur Kenntnis genommen haben. Die Behebung dieser Schwachstelle ist bereits in Arbeit.

Inhaltsverzeichnis

1	**Auftrag und Vorgehen**	**6**
1.1	Ausgangslage	6
1.2	Prüfungsziel und -fragen	6
1.3	Prüfungsumfang und -grundsätze	6
2	**Auslagerung der Informatik**	**7**
2.1	Rechtsgrundlagen der Parlamentsdienste besser dokumentieren	7
2.2	Die Auslagerung der Informatik wurde von der Verwaltungsdelegation genehmigt	7
2.3	Die Wirtschaftlichkeit der Auslagerung der Informatik wurde dargelegt	8
3	**Beschaffungen**	**9**
3.1	Die beschaffungsspezifischen Vorgaben und Prozesse sind zu verbessern	9
3.1.1	Der Support für die Beschaffungs-Beteiligten muss operativ werden	9
3.1.2	Die Prozesse und Weisungen haben grosses Verbesserungspotenzial	9
3.1.3	Die beschaffungsspezifische Ausbildung ist weiter voranzutreiben	11
3.2	Die einzelnen Beschaffungen müssen transparenter und gesamtheitlicher abgewickelt werden	11
3.2.1	Es wird Wettbewerb geschaffen, mehr wäre möglich	11
3.2.2	Zuschlagskriterien müssen wirksamer sein	12
3.2.3	Offertevaluationen müssen transparenter und qualitativ besser werden	13
3.2.4	Vertragssicherheit durch konsequente Verwendung der eigenen Vertragsvorlagen sicherstellen	14
3.2.5	Beschaffungen gesamtheitlich, ohne Splitting planen	15
3.2.6	Fehlende Transparenz bei der Dokumentation der Einzelgeschäfte	16
4	**Informatiksicherheit**	**17**
4.1	Das Netzwerk basiert auf moderner Infrastruktur	17
4.1.1	Die Ausgangslage	17
4.1.2	Das Netzwerk und die Peripherie sind für eine hohe Ausfallsicherheit gebaut	18
4.1.3	Die Umsetzung ist an der Strategie des Parlaments ausgerichtet	18
4.1.4	Die Netzwerktechnik wird gut überwacht und verwaltet	19
4.2	Die Verwaltung der Benutzer und Geräte im Parlament ist geregelt	19
4.2.1	Die Verantwortlichkeiten zwischen Parlament und Parlamentsdiensten sind geregelt	19
4.2.2	Der sicherheitstechnische Zustand der Geräte wird aktiv überwacht	20
4.2.3	Die Zugriffsrechte werden regelmässig kontrolliert	20
4.3	Das Netzwerk wird professionell überwacht und gewartet	21
4.3.1	Kontinuierliche Überwachung des Betriebes und der Sicherheit	21
4.3.2	Adäquates Change Management und Controlling	21

5	**Diverses – Abklärungen bei einzelnen Buchungen**	**22**
6	**Follow up der PA 11324 und 11461**	**22**
6.1	PA 11324 «Finanzielle Führung Beschaffungswesen und Informatik»	22
6.2	PA 11461 «Überprüfung der IT Sicherheit bei den Parlamentsdiensten»	24
7	**Schlussbesprechung**	**26**
Anhang 1:	**Rechtsgrundlagen**	**27**
Anhang 2:	**Abkürzungen, Priorisierung der Empfehlungen der EFK**	**28**

1 Auftrag und Vorgehen

1.1 Ausgangslage

Gestützt auf Artikel 6 und 8 des Finanzkontrollgesetzes (FKG) hat die Eidgenössische Finanzkontrolle im September 2014 bei den Parlamentsdiensten (PD) eine Finanzaufsichtsprüfung durchgeführt. Dabei standen die Informatik- und Beschaffungsbereiche im Fokus. Vor allem waren die Auslagerung der Informatik, die Auftragsvergaben und die Informatiksicherheit von Interesse.

1.2 Prüfungsziel und -fragen

Aus der Risikoanalyse ergaben sich folgende Prüffragen, die zu beantworten waren:

- Welches sind die technischen und finanziellen Auswirkungen der Auslagerung der Informatik, und wurden diese bei der Strategie berücksichtigt?
- Wie wurden die Beschaffungen von Gütern, Dienstleistungen und vom Personalverleih durchgeführt und wurden die entsprechenden rechtlichen Vorgaben eingehalten?
- Wie ist die Informatiksicherheit sichergestellt, speziell bei der Nutzung der persönlichen PC der Parlamentarier?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Peter Zumbühl (Revisionsleiter), Stefan Wagner und Hans-Rudolf Michel durchgeführt. Dabei hat die EFK insbesondere das Konzept und die Umsetzung der Auslagerung, des Netzwerkmanagements und -betriebs (Informatiksicherheit) sowie die Organisation, Prozesse und Vorgaben im Beschaffungsbereich sowie ausgewählte Einzelgeschäfte geprüft. Zusätzlich wurde noch der Follow up der Empfehlungen des Informatik- und Beschaffungsbereich von zwei EFK- Prüfungen (PA 11324 und PA 11461) durchgeführt.

Die Schlussfolgerungen im Bericht stützen sich auf unterschiedliche stichprobenweise durchgeführte Prüfungen von Unterlagen und basieren auf mehreren Besprechungen mit den Geprüften. Die Festlegung dieser Stichproben basiert auf dem Prinzip der Wesentlichkeit und auf Risikoüberlegungen zu den in die Prüfung einbezogenen Bereichen der Geschäftstätigkeit. Unterlagen und Auskunftserteilung.

Die notwendigen Auskünfte und Unterlagen, soweit vorhanden, hat die EFK von allen Beteiligten zeitgerecht und in zuvorkommender Weise erhalten.

2 Auslagerung der Informatik

2.1 Rechtsgrundlagen der Parlamentsdienste besser dokumentieren

Gemäss Artikel 36 der Parlamentsverwaltungsverordnung (ParlVV, SR 171.115) werden Verwaltungsverordnungen, die für die Bundesverwaltung gelten für die PD angewendet, sofern die Verwaltungsdelegation der Bundesversammlung (VD) nichts anderes bestimmt. Die VD und der Bundesrat haben die Vereinbarung vom 4. Juli 2008 über die Zusammenarbeit im Bereich des Immobilienmanagements für die Bundesversammlung und die Parlamentsdienste abgeschlossen. Darin ist z. B. auch die Zuständigkeit der VD und der PD für die Beschaffung von Informatik-, und Telekommunikationsmitteln festgehalten.

Eine vollständige Liste der entsprechenden aktuellen Vorgaben der VD stand zum Zeitpunkt der Prüfung nicht zur Verfügung. So ist z. B. die obige Vereinbarung im Intranet der PD unter den Rechtsgrundlagen nicht aufgeführt. Die EFK stellt fest, dass dadurch eine gewisse Rechtsunsicherheit besteht. Um eine umfassende Übersicht über die rechtlichen Grundlagen der PD zu gewährleisten, wäre es zweckmässig, eine vollständige Liste mit allen Vorgaben der VD zu erstellen.

Werden durch rechtsetzende Ausführungsbestimmungen dem Bundesrat oder ihm nachgeordneten Dienststellen Zuständigkeiten zugewiesen, so werden diese für die PD durch die VD oder die Generalsekretärin oder den Generalsekretär der Bundesversammlung wahrgenommen (Art. 70 Abs. 3 Parlamentsgesetz). In diesem Sinne erfolgt die in der Org-VöB vorgesehene Information über die getätigten Beschaffungen nicht an das Bundesamt für Bauten und Logistik sondern an die VD.

Empfehlung 1 (Priorität 2)

Die EFK empfiehlt den Parlamentsdiensten eine Liste aller für sie massgebenden Rechtsgrundlagen inklusive aller entsprechenden Vorgaben der Verwaltungsdelegation zu erstellen und diese auf dem aktuellsten Stand zu halten.

Stellungnahme der PD:
Einverstanden. Eine erste Version einer solchen "Weisungssammlung" wird erarbeitet und bis zum 30.06.2015 mindestens mit den GL- und VD-Entscheiden ab 2014 erstellt werden.

2.2 Die Auslagerung der Informatik wurde von der Verwaltungsdelegation genehmigt

Die Parlamentsdienste (PD) orientierten die Verwaltungsdelegation der eidgenössischen Räte (VD) mit Brief vom 18. Oktober 2010, dass sie mit dem Bundesamt für Informatik und Telekommunikation (BIT) als Dienstleistungserbringer nicht zufrieden seien. Die PD zeigten drei Alternativen auf:

- mit der Variante «BIT als Dienstleistungslieferant»;
- der Variante «Externe Firma/Firmen» und
- der Variante «Insourcing zu den PD».

Es wurden für alle Varianten die Betriebs- und Unterhaltskosten ermittelt und soweit erforderlich auch die einmaligen Umstellungskosten. Die Kostenberechnung der PD zeigte, dass die Variante «Externe Firma/Firmen» trotz Umstellungskosten die Kostengünstigste war, während die BIT-Lösung massiv teurer war. Die VD genehmigte gemäss Protokoll ihrer Sitzung vom 12. November 2010 die Kündigung der BIT Verträge und die öffentliche Ausschreibung dieser Dienstleistung im Frühjahr 2011.

Die Auslagerung wurde damit von der zuständigen Stelle genehmigt. Die EFK hat zur Genehmigung der Auslagerung grundsätzlich keine Bemerkungen.

2.3 Die Wirtschaftlichkeit der Auslagerung der Informatik wurde dargelegt

Die der VD vorgelegten Kosten der verschiedenen Varianten für den Betrieb der IKT Basisinfrastruktur zeigten, dass die Auslagerung der Informatik mit den einmaligen Umstellungskosten und den jährlichen Betriebs- und Unterhaltskosten von rund 893'000 Franken die günstigste Lösung war.

Die aktuell für das Jahr 2014 massgebenden Betriebs- und Unterhaltskosten wurden von den PD mit rund 1'395'000 Franken beziffert. Als Gründe für die Erhöhung gegenüber den im Variantenvergleich dargelegten Kosten wurden z. B. «zusätzliche Sicherheitsmassnahmen» und «zusätzliches Management-Netz für die Rechencenter-Infrastruktur» aufgeführt. Ausgehend von diesen Beträgen, die von der EFK nicht speziell geprüft wurden, kann der Schluss gezogen werden, dass im Vergleich zu den ursprünglichen Werten trotz nun höheren Betriebs- und Unterhaltskosten sich keine andere Variante als die wirtschaftlich günstigere präsentiert.

Die EFK hält fest, dass die Umsetzung der Auslagerung aus technischer Sicht (Netzwerke und Netzwerkbetrieb, Überwachung und Aktualisierung, Firewall) an den Auftragnehmer gut verlief. Nach Durchsicht der vorhandenen Projektdokumentation kommt die EFK zum Schluss, dass das Projekt zwar nicht buchstabengetreu nach Hermes aber doch sinngemäss und gut kontrolliert umgesetzt wurde. Gegenüber der BIT Lösung konnte durch die neue Technik unter anderem die Übertragungskapazität erhöht werden.

Genauer untersucht wurde von der EFK die entsprechende Auftragsvergabe «Betrieb IKT Basis Infrastruktur für Parlamentsdienste», die einige Mängel zeigte (siehe drittes Kapitel). Der Auftrag wurde Ende 2011 erteilt und mit einigen Zusatzverträgen ergänzt. Bei wiederkehrenden Leistungen dürfen gemäss Artikel 15a VöB Verträge für höchstens 5 Jahre abgeschlossen werden. Eine Neuausschreibung dieses Mandats ist deshalb rechtzeitig zu planen (vgl. Empfehlung 6).

3 Beschaffungen

3.1 Die beschaffungsspezifischen Vorgaben und Prozesse sind zu verbessern

3.1.1 Der Support für die Beschaffungs-Beteiligten muss operativ werden

Aufgrund der Empfehlung der EFK bei der letzten Beschaffungsprüfung bei den PD (PA 11324) wurden die IT Beschaffungen zentralisiert. In den Vorgaben „Beschaffungs- und Vertragswesen" im Intranet wird auf eine interne Ansprechperson als Unterstützung für Beschaffungs-Beteiligte hingewiesen. Der Mitarbeiter, der diese Funktion wahrnahm, hat in der Zwischenzeit die PD verlassen. Dieser Support wurde jedoch nicht in die Prozesse eingebunden, auch fehlen in den beschaffungsspezifischen Regelwerken entsprechende Pflichten, Aufgaben und Kompetenzen. Dieser Support wurde zwar geschaffen, aber operativ ist er deshalb nicht. Die PD bestätigte, dass diese Aufgabe neu dem Bereich «Sicherheit und Projektmanagement» zugeordnet wird.

Eine gut funktionierende Beschaffungsorganisation mit in die Prozesse eingegliederten, bereits bestehenden Support für die Beschaffungs-Beteiligten mit dem nötigen Beschaffungs-Knowhow ist für die PD von grosser Bedeutung. Damit können die im Rahmen dieser Prüfung festgestellten Mängel rasch behoben werden und die PD kann künftig effizienter und transparenter beschaffen.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten eine gut funktionierende Beschaffungsorganisation sicherzustellen und auch den Support für die Beschaffungs-Beteiligten rasch in die Prozesse einzubinden, ihre Aufgaben, Pflichten und Kompetenzen rasch zu regeln das nötige Beschaffungs-Know-how sicherzustellen.

Stellungnahme der PD:
Einverstanden. Die Beschaffungsorganisation der Parlamentsdienste ist definiert. Sie wird nun noch so weit als notwendig dokumentiert. Die Zusammenarbeit mit dem BBL wird wie bisher weiter gepflegt. Das ungenügende vertragsjuristische Know-how soll durch externe Unterstützung, insbesondere mit dem BBL, gegebenenfalls mit Dritten sichergestellt werden. Die Parlamentsdienste sind zu klein, um alles selber machen zu können.

3.1.2 Die Prozesse und Weisungen haben grosses Verbesserungspotenzial

Bei den PD ist unter dem Titel «Beschaffungs- und Vertragswesen» eine Auflistung aller Rechtsgrundlagen im Beschaffungsbereich, wie u.a. auch die unten aufgeführten Formulare im Intranet verfügbar. Es wird auch darauf hingewiesen, dass eine interne Ansprechperson die Beschaffungs-Beteiligten unterstützt.

Als beschaffungsspezifische Vorgaben gibt es das Prozessschema, das Laufblatt für Beschaffungen, die Checkliste Beschaffungsverfahren und das Dokument Beschaffungsprozess. Alle diese Formulare sind nicht aufeinander abgestimmt. Insbesondere die Terminologie der Verantwortlichkeiten ist je nach Dokument unterschiedlich. So ist z. B. im Dokument «Beschaffungsprozess» alle Verantwortlichkeiten von Bedürfnis bis Vertragsentwurf dem Dienstchef zugewiesen, nur diese Funktion findet sich weder im Laufblatt noch im Prozessschema.

Auch haben alle bestehenden Dokumente weiteres Verbesserungspotenzial.

Prozessschema:
Der Beschaffungsprozess ist im Wesentlichen nur abgebildet durch Offertanfrage und Prüfen der Offerte. Wesentliche Elemente des Beschaffungsprozesses wie z. B. Wahl des Beschaffungsverfahrens, erstellen des Evaluationsberichtes usw. fehlen jedoch. Auch wäre es zweckmässig wenn nicht nur die Verantwortlichkeiten aufgeführt wären sondern auch, wer in der entsprechenden Phase z. B. miteinbezogen und informiert werden soll und wer was kontrolliert. Sehr dienlich wäre auch, wenn in den einzelnen Phasen festgehalten wäre, was die entsprechende Tätigkeit beinhaltet. Ein Link mit Verweis auf dafür massgebende Dokumente könnte sehr unterstützend sein. Auch der Support der Beschaffungs-Beteiligten muss, gemäss ihren Aufgaben und Kompetenzen, darin abgebildet werden.

Dokument Beschaffungsprozess:
Unter «Hilfsmittel/Bemerkungen» sind gewisse Hinweise aufgeführt. Es wäre zweckmässig, wenn in den einzelnen Phasen auf detailliertere Hilfsmittel hingewiesen wird wie z. B. einzelne Beschaffungsverfahren und was dabei zu beachten ist. Solche Dokumente sollten auch verlinkt sein. In diesem Dokument fehlt auch jeglicher Hinweis auf den Support der Beschaffungs-Beteiligten.

Auch ist unter Pkt. 15 «Ablage der Vertragsurkunde und aller beschaffungsrechtlichen Dokumente....» festgehalten, dass die Aufbewahrungsfristen mindestens drei Jahre ist bzw. bis zur nächsten Revision der EFK. Diese drei Jahre, wie sie in der Org-VöB festgehalten und auch für die PD zweckmässig ist, gilt nur für Konkurrenzofferten, Arbeitspapiere usw. nicht aber für die Verträge deren Aufbewahrungsfrist gemäss OR mindestens 10 Jahre beträgt. Die Aufbewahrungsfrist von mindestens drei Jahren ist absolut, ohne Einschränkung «bis zur nächsten Revision der EFK», wie im Dokument aufgeführt ist.

Checkliste Beschaffungen:
Auf diesem Dokument fehlt das Feld für den Eintrag, um welches Beschaffungsgeschäft es sich im konkreten Fall handelt. Es wäre auch zweckmässig, wenn daraus ersichtlich ist, ob es sich um einen Erstauftrag oder um einen Folgeauftrag handelt. Unter «Voraussetzung für freihändiges Verfahren» kann «ja/nein» angekreuzt werden, welche Ausnahmebestimmung nach Art. 13 VöB massgebend ist. Es fehlt jedoch das Feld «Begründung» denn die Transparenz kann nur sichergestellt werden, wenn auch klar begründet ist, warum das entsprechende Geschäft diesem Ausnahmeartikel entspricht. Unter «Einladungsverfahren» muss bestätigt werden, dass mindestens drei Offerten eingeholt wurden. Es genügt nicht, wenn in der Checkliste überprüft wird, dass mindestens drei Angebote eingeholt wurden. Auch bei den im Einladungsverfahren vergebenen Aufträgen muss ein Evaluationsbericht erstellt werden, der sich zur Bewertung der vorgängig definierten Zuschlagskriterien und somit zum wirtschaftlich günstigsten Angebot äussert. Das Erstellen eines Evaluationsberichtes über die Bewertung der Zuschlagskriterien mit der Bestimmung des wirtschaftlich günstigsten Angebotes sollte als Checkpunkt im Formular enthalten sein.

Laufblatt für Beschaffungen:
In diesem Laufblatt sind die Verantwortlichkeiten, zu erstellende Dokumente, Visum mit Datum aufgeführt. Verantwortlich für die Verfahrenswahl ist der Antragsteller, der Support der Beschaffungs-Beteiligten ist auch in diesem Dokument nicht aufgeführt. Gemäss diesem Laufblatt muss das zuständige Geschäftsleitungsmitglied in der Phase Vergabe/Zuschlag erstmals visieren. Der

Einbezug dieses Geschäftsleitungsmitglieds zu diesem Zeitpunkt ist zu spät. Derjenige der mit der Unterschrift die Verantwortung trägt muss zu Beginn, spätestens bei Bedürfnis/Verfahrenswahl beigezogen werden, denn dort werden die Meilensteine gesetzt. Positiv zu erwähnen ist, dass das Erstellen von Unbefangenheitserklärungen im Laufblatt integriert ist.

Die vorgängig aufgeführten Dokumente sind dementsprechend zu verbessern; allenfalls ist das Dokument Beschaffungsprozess mit dem Prozessschema zu verschmelzen und die PD spezifischen Beschaffungsvorgaben wie z. B. Aufgaben, Pflichten und Kompetenzen des Supports der Beschaffungs-Beteiligten ist z. B. in einem Beschaffungshandbuch zu regeln.

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten, die Beschaffungsdokumente aufeinander abzustimmen, zu ergänzen und die Beschaffungsvorgaben wie z. B. Aufgaben, Pflichten und Kompetenzen des Supports für die Beschaffungs-Beteiligten sowie wer in den einzelnen Prozessschritten mit einbezogen resp. informiert werden muss und wer was kontrolliert, darin zu integrieren. Im Weiteren sind die Dokumente Beschaffungsprozess und Prozessschema miteinander zu verschmelzen.

Stellungnahme der PD:
Einverstanden.

3.1.3 Die beschaffungsspezifische Ausbildung ist weiter voranzutreiben

Der für den Support für die Beschaffungs-Beteiligten zuständige Mitarbeiter der PD, der über das nötige Beschaffungs-Know-how verfügte, hat die PD verlassen. Dieser Mitarbeiter hat alle bei Beschaffungen involvierte Mitarbeitende der PD im Rahmen einer kurzen Einführung entsprechend sensibilisiert.

Es ist zwingend notwendig, dass das entsprechende Know-how durch die nun zuständige Stelle «Sicherheit und Projektmanagement» rasch aufgebaut wird und ihr Wissen allen bei den Beschaffungen der PD involvierten Mitarbeitenden bedarfskonform weitergegeben wird (vgl. Ziffer 3.1.1).

3.2 Die einzelnen Beschaffungen müssen transparenter und gesamtheitlicher abgewickelt werden

Die EFK hat elf, teilweise mehrjährige Geschäfte von insgesamt rund 4 Mio. Franken geprüft. Das jährliche Finanzvolumen beträgt rund 8,8 Mio. Franken.

3.2.1 Es wird Wettbewerb geschaffen, mehr wäre möglich

Drei der geprüften Geschäfte, darunter ein «Personalverleih» wurden aufgrund einer öffentlichen Ausschreibung vergeben. Zwei Beschaffungen wurden im Einladungsverfahren durchgeführt. Bei zwei weiteren war dasselbe Verfahren vorgesehen, eines wurde jedoch aufgrund geänderter finanziellen Rahmenbedingungen abgebrochen und das andere ist noch in der Grobkonzeptphase.

Zur Verfahrenswahl dieser, im Wettbewerb vergebenen Aufträgen, gibt es keine Bemerkungen.

Die restlichen Aufträge wurden freihändig vergeben. Es sind oft wiederkehrende Aufträge, die halb- oder ganzjährlich abgeschlossen wurden. Bei den freihändig vergebenen, wiederkehrenden Aufträgen gibt es Verbesserungspotenzial, es hätte mehr Wettbewerb geschaffen werden können (vgl. Ziffer 3.4.5; «Splitting bei wiederkehrenden Aufträgen»).

3.2.2 Zuschlagskriterien müssen wirksamer sein

Zu den Pflichtenheften der drei öffentlich ausgeschriebenen Aufträge gibt es insbesondere hinsichtlich des Zuschlagskriteriums «Preis» Bemerkungen anzubringen. Bei der Beschaffung der «Wartung und Weiterentwicklung von IT Spezialanwendungen der PD, Los 2» wurden für den Preis fünf verschiedene Zuschlagskriterien definiert. Bei drei dieser Zuschlagskriterien hat ein Bewerber null Franken offeriert. Das hat zur Folge, dass jeder andere Bewerber, egal welchen Betrag er einsetzt, null Punkte erhält. Im konkreten Fall sind davon 43% aller möglichen Preis-Bewertungspunkte betroffen.

Im Pflichtenheft für den «Betrieb Basis Infrastruktur für PD» wurden 17 Preiselemente einzeln bewertet. Auch hier wurde bei einem Kostenelement von einem Bewerber null Franken eingesetzt. Das «wirtschaftlich günstigste Angebot» hatte bei 11 Positionen 0 Punkte erhalten und insgesamt nur 44% der möglichen Punktzahl erreicht, obwohl bei den nichtmonetären Kriterien der Zuschlagsempfänger das Punktemaximum erhielt. Bei den Preisen für die Kosten LAN und WLAN ist klar ersichtlich, dass Bewerber taktierten. So wurden beispielsweise die einmaligen Kosten sehr hoch eingesetzt und die wiederkehrenden Kosten, die insgesamt achtmal höher gewichtet wurden, sehr tief.

Die Preisbewertungsmodelle dieser beiden Geschäfte öffnen das Tor zum taktieren. Somit wird zwar das arithmetisch beste Angebot ermittelt, nicht aber zwingend das wirtschaftlich Günstigste. Deshalb können diese Modelle nicht empfohlen werden.

Auch das beim Personalverleih angewendete, asymptotische Preisbewertungssystem ist nicht geeignet, denn diejenige Offerte mit doppeltem Preis – gegenüber dem tiefsten Offertpreis – erhält immer noch 50% der Punkte und diejenige mit dem vierfachen Offertpreis immer noch 25%. Bei diesem Modell gibt es also «gratis» Punkte und somit wird die Gewichtung des Preises de facto reduziert.

Zuschlagskriterien wie «Bestätigung, dass der Anbieter mindestens 3 Entwickler hat...» sind nicht geeignet. Hier wird die Eignung des Anbieters bewertet und nicht, dass dieser den konkreten Auftrag am Wirtschaftlichsten ausführen kann. Dieses Kriterium ist nicht auftragsbezogen formuliert, denn der Anbieter verpflichtet sich mit der gewählten Formulierung nicht, die Entwickler auch für dieses Projekt einzusetzen (Empfehlungen siehe Kapitel 3.2.3).

3.2.3 Offertevaluationen müssen transparenter und qualitativ besser werden

Bei der Offertevaluation für die Beschaffung des Personalverleihs wurde das Zuschlagskriterium 02 fälschlicherweise mit null Punkten bewertet, obwohl vermerkt ist, dass alle Ausbildungen vorhanden sind. Mit dem dafür eigentlich zustehenden Punktemaximum bei diesem Kriterium wäre dieses Angebot das wirtschaftlich Günstigste gewesen und die Firma hätte für das Los 3+4 den Zuschlag erhalten müssen. Beim selben Geschäft wurde bei mehreren Zuschlagskriterien festgehalten, dass die Überprüfung der Selbstdeklaration vorbehalten ist. Ob eine Überprüfung stattgefunden hat ist nicht dokumentiert.

Im Entwurf des Evaluationsberichtes für den «Betrieb IKT Basis Infrastruktur für PD» war der Preis für das Kriterium P 3.1 32'068 Franken. Es gab Nachverhandlungen. Gemäss dem nicht unterschriebenen Evaluationsberichtes erhöhte sich dieser Betrag auf 606'000 Franken. Es ist festgehalten, dass dieser Evaluationsbericht die Ergebnisse der Nachverhandlungen mitberücksichtigt. Nur bei 7 der 17 Preispositionen entsprechen die in diesem Evaluationsbericht festgehaltenen Preise denjenigen der Nachverhandlungen und den in die Verträge eingeflossenen Preise. Die für die Evaluation berücksichtigten Preise sind teilweise falsch und deren Herkunft nicht nachvollziehbar. Das wirtschaftlich günstigste Angebot wurde aufgrund falscher Offertpreise ermittelt. Mit den «richtigen Preisen» hätte es aber keine andere Rangfolge gegeben.

In den Ausschreibungsunterlagen ist die Abstufung der Bewertungen enthalten, in der Offertevaluation beim selben Geschäft ist jedoch oft nicht oder zu wenig klar aufgeführt, aus welche Gründen Abzüge gemacht werden mussten. Ein Hinweis «qualitativ ungenügend» reicht nicht um Transparenz zu schaffen. Es muss aufgeführt werden was fehlt, warum es qualitativ ungenügend ist.

Korrekterweise wurden auch bei den Geschäften, die im Einladungsverfahren vergeben wurden, Evaluationsberichte erstellt. Beim Geschäft «Einführung IT Service Management mit «Helpline» beim DINT» gibt es folgende Mängel:

- Aus dem Berichtsdeckblatt ist der Evaluationsgegenstand nicht ersichtlich.
- Die Bewertungskriterien inklusive Kosten sind als Eignungskriterien anstatt als Zuschlagskriterien deklariert.
- Es wurden 13 Kriterien bewertet, die Bewertung ist nicht begründet.
- Das Preisbewertungsmodell ist nicht ersichtlich, auch nicht, wie die offerierten Preise auf die beiden Zuschlagskriterien «Kosten Lizenzen, ASP, Betriebsaufwand» und «Einführungskosten, Projektunterstützung» aufgeteilt wurden.

Beim Geschäft «Aktualisierung der Multimedia Investition für das Politforum im Käfigturm» wurde ein kleiner Evaluationsbericht erstellt. Der Offertsteller mit dem tiefsten Preis erhielt den Zuschlag. Daraus kann der Schluss gezogen werden, dass der Preis das einzige Kriterium war. Die Gleichbehandlung aller Anbieter kann nur sichergestellt werden, wenn die Zuschlagskriterien auch bei Einladungsverfahren vorgängig festgelegt und dokumentiert werden.

Empfehlung 4 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten, in der Wettbewerbsphase Folgendes zu verbessern:

- *In den Ausschreibungsunterlagen sind die Zuschlagskriterien auftragsbezogen zu formulieren und es ist nur der Gesamtpreis zu bewerten. Das anzuwendende Preisberechnungsmodell ist auftragsspezifisch festzulegen, wobei das asymptotische ohne Potenzierung nicht geeignet ist.*
- *Bei den Offertevaluationen ist sicherzustellen, dass diese transparent und nachvollziehbar die einzelnen Schritte festhalten und mit einer funktionierenden Qualitätssicherung die Richtigkeit garantieren.*
- *Auch bei Vergaben im Einladungsverfahren sind die Zuschlagskriterien vorgängig festzulegen und zu dokumentieren.*

Stellungnahme der PD:

Grundsätzlich einverstanden. Die PD behalten sich vor, im Rahmen des gesetzlichen Rahmens ihren Spielraum auszunutzen. Die Zusammenarbeit mit dem BBL wird wie bisher weiter gepflegt. Die Empfehlung wird ab sofort im Einzelfall geprüft werden.

3.2.4 Vertragssicherheit durch konsequente Verwendung der eigenen Vertragsvorlagen sicherstellen

Mit Ausnahme des Auftrages «Betrieb IKT Basis Infrastruktur für PD» wurden richtigerweise alle geprüften Aufträge mit den eigenen Vertragsvorlagen abgeschlossen. Bei dieser Ausnahme wurde der Vertrag auf dem Formular des Beauftragten abgeschlossen. Das Vertragsdokument regelt viele Elemente, die auch in den AGB des Bundes geregelt sind. In Ziffer 2 des Vertrages steht: «Dieser Vertrag regelt die Grundsätze» und auch «im weiteren sind die AGB des Bundes anzuwenden». Das heisst, dass zuerst dieses Dokument mit den Bestimmungen des Beauftragten und erst subsidiär die AGB des Bundes Gültigkeit haben. Aufgrund dieses Vertrages wurden insgesamt 18 weitere Verträge abgeschlossen, alle ebenfalls auf Vertragsgrundlagen des Beauftragten. Beim Auftrag «Switches im Media RZ» wurde die unterschriebene Offerte nach Unterschrift der PD direkt zum Vertrag. In diesem Vertrag ist als Vertragsbestandteil folgendes definiert: «auf diese Leistungen und die zugehörenden Vertragsbestandteile finden die Allgemeinen Geschäftsbedingungen für Geschäftskunden Anwendung», also die AGB des Beauftragten. Aufgrund dieser Vertragsbestimmungen gelten die AGB des Bundes, wenn überhaupt nur subsidiär. Um die Vertragssicherheit sicherzustellen sind grundsätzlich die Verträge auf den Vertragsvorlagen der PD mit den AGB des Bundes abzuschliessen. Die AGB des Beauftragten sind dabei weg zu bedingen.

Im Vertrag «Einführung IT Service Management mit «Helpline» beim DINT» gibt es widersprüchliche Regelungen. So endet die Leistungserbringung gemäss Vertrag am 31. Dezember 2013, also rund ein halbes Jahr nach Unterzeichnung, obwohl der Auftrag auch die «helpline Professional Implementation inkl. 3 Jahre Software Pflege» vorsieht.

Auch werden einzelne Verträge erst verspätet, Monate nach Beginn der Leistungserbringung unterzeichnet.

Empfehlung 5 (Priorität 2)

Die EFK empfiehlt den Parlamentsdiensten die Vertragssicherheit zu stärken, die Verträge vor Beginn der Leistungserbringung abzuschliessen und grundsätzlich auf den Vertragsvorlagen der Parlamentsdienste mit den AGB des Bundes zu basieren. Die AGB des Beauftragten sind weg zu bedingen.

Stellungnahme der PD:
Einverstanden. Bereits bisher wurden die AGB der Beauftragten wegbedungen und nur in Ausnahmefällen akzeptiert.

3.2.5 Beschaffungen gesamtheitlich, ohne Splitting planen

Einige der geprüften Verträge werden halbjährlich oder jährlich abgeschlossen, jeweils basierend auf einer neuen Offerte. Für die «Einführung ITSM und Coaching des neuen Betriebsleiters» wurden z. B. halbjährige Verträge abgeschlossen. Das Auftragsvolumen beträgt gemäss Laufblatt und Bestell- und Vertragsliste 198'000 Franken, die Summe der beiden Halbjahresverträge beträgt zusammen 231'000 Franken. In der undatierten Checkliste wird aufgeführt, dass der Auftrag nicht aufgeteilt wurde, um den Schwellenwert zu umgehen. Aus der Checkliste ist nicht ersichtlich, ob sich diese auf den ersten Vertrag oder den zweiten Vertrag des Jahres beziffert. Die freihändige Vergabe wurde begründet, mit «Leistungen zur Ersetzung, Ergänzung oder Erweiterung bereits erbrachter Leistungen müssen dem ursprünglichen Anbieter oder der ursprünglichen Anbieterin vergeben werden, weil einzig dadurch die Austauschbarkeit mit schon vorhandenem Material oder Dienstleistungen gewährleistet ist». Das ist der entsprechende Text der Verordnung und legt nicht dar, warum dieses Geschäft diesem Text entspricht.

Auch die Wartung und der Support im Jahr 2014 für die beiden Bereiche «Intra-, Internet» und «ELAN und ELAS» wurden mit Jahresverträgen freihändig vergeben. Begründet wurden diese freihändigen Vergaben mit «Folgeauftrag, Schutz des geistigen Eigentums» respektive «Folgeauftrag, Spezialwissen und Fach Knowhow für Wartung und Support von Individualsoftware» Auch diese Formulierungen begründen eine freihändige Vergabe nicht.

Zahlreiche Aufträge wurden gesplittet und mit Halb- oder Jahresverträgen abgeschlossen. Grundsätzlich sind Aufträge gesamtheitlich zu planen. Aufträge, die sich über mehrere Jahre erstrecken sind nach dem für das ganze Auftragsvolumen massgebenden Vergabeverfahren abzuwickeln. Allfällig spätere Phasen können optional ausgeschrieben und ins Vertragswerk aufgenommen werden.

Werden freihändige Vergaben getätigt obwohl vom Volumen her Wettbewerb geschaffen werden müsste, so sind diese gemäss Artikel 13 VöB zu begründen. Dabei genügt nicht, wie teilweise praktiziert, den Verordnungstext abzuschreiben, sondern es muss begründet werden, warum diese konkrete Beschaffung diesem Ausnahmeartikel entspricht.

Empfehlung 6 (Priorität 1)

Die EFK empfiehlt den Parlamentsdiensten Beschaffungen mehrjährig ganzheitlich zu planen. Dabei ist das ganze Auftragsvolumen inklusive allfälliger Optionen für die Wahl des Beschaffungsverfahrens massgebend. Sind freihändige Vergaben bei Auftragsvolumen, die ein Einladungsverfahren oder eine öffentliche Ausschreibung erfordern würden geplant, so ist klar zu begründen, warum dieses konkrete Geschäft dem Ausnahmeartikel des VöB entspricht.

Stellungnahme der PD:
Grundsätzlich einverstanden. Dies wurde bereits mittels des 2012 eingeführten Projektportfolios und der 2014 verabschiedeten IS-Governance formalisiert. Allerdings ist eine Planung im Umfeld des Parlamentes nur beschränkt möglich.

3.2.6 Fehlende Transparenz bei der Dokumentation der Einzelgeschäfte

Die Nachvollziehbarkeit der geprüften Geschäfte war erschwert, weil mehrere Dokumente, die für die Nachvollziehbarkeit zwingend erforderlich wären nicht beigebracht werden konnten. So waren die Offertevaluationen der drei im öffentlichen Verfahren vergebenen Aufträgen bei den PD nur im Entwurf vorhanden. Ein unterschriebener Evaluationsbericht konnten vom Bundesamt für Bauten und Logistik geliefert werden, die entsprechenden Berichte der Geschäfte «Betrieb IKT Basis Infrastruktur für PD» und «Personalverleih» liegen nur in einem Entwurf vor. Bei diesen ist nicht klar, ob das die finale Fassung war. Beim ersten dieser Beiden ist die Herkunft der bewerteten Preise nicht nachvollziehbar.

Bei den uns aus dem Dokumentensystem abgegebenen Laufblättern fehlen in der Regel die entsprechenden Unterschriften. Sie sollen mit dem unterschriebenen Vertrag anderswo abgelegt sein. Unterschriebene Laufblätter wurden nicht vorgelegt.

Ebenfalls zu bemängeln ist, dass meistens ein Hinweis fehlt, wenn ein neu abgeschlossener Vertrag ein Folgeauftrag ist. Dadurch fehlt eine gesamtheitliche Sicht vom ursprünglichen Initialvertrag, dem entsprechenden Vergabeverfahren und den Nachträgen. Die Transparenz wird auch beim, ab Januar 2015 eingeführten Vertragsmanagement Bund nicht wesentlich besser, wenn jeder Folgeauftrag als «neuer», selbständiger Vertrag erfasst wird.

In der Dokumentenablage der PD gibt es folgende Struktur: «Arbeitsrapporte», «Bestellung», «Korrespondenz», «Lizenz-, Garantie- und Wartungsdokumente», «Offerte/Projektdokumente», «Rechnungen», «Vertrag» und «Vertrag unterzeichnet». Diese Struktur ist nicht Prozess orientiert sondern alphabetisch gegliedert. Auch fehlen beschaffungsspezifische Elemente wie Bedarf, Ausschreibung, Offertevaluation usw. Wohl aufgrund mangelnder Vorgaben sind zahlreiche Dokumente, die für die Nachvollziehbarkeit der Geschäfte zwingend notwendig sind in ihrer definitiven Fassung nicht verfügbar.

Auch die Bestell- und Vertragsliste zeigt Mängel auf. So wurden die zwei Geschäfte «Wartung und Support ELAN und ELAS 2014» sowie «Wartung und Support verbalix 2014» doppelt erfasst; einmal als Investition und einmal als Betrieb, wobei das erste Geschäft sogar mit unterschiedlichen Beträgen. Die PD betätigen, dass effektiv nur ein Vertrag besteht.

Empfehlung 7 (Priorität 2)

Die EFK empfiehlt den Parlamentsdiensten, die Ablagestruktur prozessorientiert so aufzubauen, dass auch die beschaffungsspezifischen Elemente abgebildet werden. In der Beschaffungsdokumentation ist auch festzuhalten, was in welchem Ablageelement in welcher Form abzulegen ist, damit die Nachvollziehbarkeit der Beschaffung sichergestellt werden kann.

Stellungnahme der PD:
Grundsätzlich einverstanden. Die Parlamentsdienste verstehen darunter minimal die Trennung zwischen "Beschaffungsphase" (Ausschreibung) und "Betriebsphase" (nach Zuschlag). Die konkrete Lösung wird erarbeitet und bis Ende 2015 eingeführt, sodass spätestens ab 01.01.2016 die Dokumente darin abgelegt werden können.

4 Informatiksicherheit

Die Fragestellung lautete: Wie ist die Informatiksicherheit sichergestellt insbesondere bei der Nutzung durch die Parlamentarier mit ihren eigenen Geräte sowie mit dem Wechsel zum externen Leistungserbringer (LE).

Die Prüfung der Informatiksicherheit fokussierte sich auf das Netzwerkmanagement und den Netzwerkbetrieb welche die Bundesversammlung (PARL) sowie die Parlamentsdienste nutzen und im Zusammenhang mit dem Wechsel vom BIT zum externen LE stehen.

4.1 Das Netzwerk basiert auf moderner Infrastruktur

4.1.1 Die Ausgangslage

Mit der Weiterentwicklung der Basisinfrastruktur entschied die VD die Aufgaben mit einer WTO Ausschreibung einem neuen LE anzuvertrauen. Man erhoffte sich einen günstigeren Betrieb ab 1. Januar 2012, welcher insbesondere die Datennetzwerke und Telekommunikationsinfrastruktur beinhalteten sollte. Das Augenmerk legte man auf die Interoperabilität (Daten- und Dokumentenaustausch sowie Zugriffe auf IKT-Systeme) zwischen Parlamentsdiensten und den Verwaltungen, der IT-Sicherheit im Allgemeinen und der Ausbaufähigkeiten für neue Technologien (Voip[1], Mobiledevices, etc.).

PARL verfügt heute über einen autonomen Informatikdienst und eine eigene IKT-Infrastruktur. Der «Dienst für Informatik und neue Technologien» (DINT) der PD ist für die IKT-Basisinfrastruktur (Netzwerkkomponenten, Verwaltung und Betrieb der Netze, inkl. Helpdesk) zuständig. Er führt den LE hinsichtlich des Netzwerkmanagements und gewährleistet den Netzwerkbetrieb. Via Tasksourcing[2] hat der DINT die Verwaltung der Infrastruktur an einen externen Leistungserbringer (LE)

[1] engl. «Voice over IP», Telefonie mit und ohne Video welche über das Datennetz übertragen werden (wie z. B. Skype)

[2] Eine Form des Outsourcings bei der das Bereitstellen von Ressourcen und Tools durch den Dienstleister erfolgt, die Erfüllung von IKT-Aufgaben verbleibt beim Kunden.

übertragen. Die Gebäudeverkabelung sowie Server-, Client- und Datenspeichersysteme gehörten nicht zum Umfang des vergebenen Auftrages. Das BIT ist verantwortlich für den Netzübergang in die Bundesverwaltung und stellt in den Parlamentsgebäuden den WLAN Zugang «public» und «private» der Bundesverwaltung zur Verfügung.

4.1.2 Das Netzwerk und die Peripherie sind für eine hohe Ausfallsicherheit gebaut

Das gesamte Netzwerk besteht heute aus vier physisch getrennten Netzwerken. Jedes physische Netzwerk beinhaltet mehrere logisch aufgeteilte Netzwerke. Physisch getrennt heisst, dass die Verkabelungen der Gebäude in separaten Trassen geführt werden. Die Ratsmitglieder inkl. WLAN-Hotspots, die Parlamentsdienste, die Infrastruktur (z. B. www.parlament.ch, etc.) und das Management-Netzwerk haben jeweils eine eigene Basisinfrastruktur. Jedes Netzwerk ist in sich Redundant und funktioniert selbständig.

Logisch getrennt heisst, dass die bereitgestellten Dienste (Anwendungen wie Mail, Dateiablagen, Web-Auftritten, Drucker, VoIP Telefonie) und Arbeitsplätze pro Standort jeweils organisatorisch und zugriffsgesteuert zur Verfügung gestellt werden.

Das Netz der PD ist am besten gesichert. Es sind zahlreiche Sicherheitsmassnahmen implementiert und die Aktivitäten der Benutzer sind nachvollziehbar. Zertifikate für die Authentifizierung und Zertifikate für den Zugang und den Datenaustausch unter den Geräten sind Standard.

4.1.3 Die Umsetzung ist an der Strategie des Parlaments ausgerichtet

Das Informatikkonzept der Bundesversammlung (Beschluss der Verwaltungsdelegation vom 12. November 2010) und die Strategie 2012 – 2016 vom 30. April 2012, genehmigt durch die Verwaltungsdelegation, bilden die Grundlage für die Infrastruktur.

Der Generalsekretär hat sowohl die Weisung über die Informatiksicherheit in den Parlamentsdiensten (WIsPD) vom 26. März 2012 erlassen sowie die Regeln zur Governance der Informationssysteme der Bundesversammlung (IS-Governance) am 1.September 2014 in Kraft gesetzt. Auf diesen Rahmenbedingungen basierend hat der DINT die Informatikstrategie in Form einer Roadmap definiert. Die IT-Infrastruktur/Ausrüstung sowie die Datenkommunikations-Dienstleistungen für die Ratsmitglieder der 49. Legislatur (2013-2015) wurden festgelegt und am 16. Oktober 2012 von der Verwaltungsdelegation verabschiedet.

Aus Sicht der EFK wurden die Vorgaben aus Strategie und Konzept der Verwaltungsdelegation weitgehend umgesetzt. Durch den Generalsekretär ist der notwendige Rahmen erstellt worden. Innerhalb dieses Rahmens hat der DINT eine sinnvolle Lösung aufgebaut. Alle wesentlichen Punkte aus der Weisung des Bundesrats über IKT-Sicherheit in der Bundesverwaltung wurden ebenfalls abgedeckt. Der abgegrenzte Bereich für die Parlamentsdienste und die definierte Übergabeschnittstelle von Dokumenten und Informationen zwischen den Parlamentsdiensten und dem Parlament ermöglichen beiden Seiten einen ihren Sicherheitsvorstellungen entsprechenden Betrieb.

4.1.4 Die Netzwerktechnik wird gut überwacht und verwaltet

Die Infrastruktur der vier Netze besteht aus meist doppelten Verkabelungen und Netzwerkgeräten. Für die Sicherstellung der Verfügbarkeit der Infrastruktur überwacht das Network Operation Center (NOC) des externen LEs das Funktionieren der eingesetzten Geräte. Überwacht werden insbesondere die Aktivitäten auf dem Netzwerk, die Qualität und Kapazität der Netzwerkdienste, aber auch die Konfiguration beim Austausch von Geräten. Basis bilden die Normen ISO 27000[3] über die Informatiksicherheit sowie IT Infrastructure Library[4] (ITIL) zur Umsetzung eines IT-Service-Managements (ITSM).

Der Servicezugang des Leistungserbringers erfolgt über LAN-Interconnect Services auf alle im Netzwerkverkehr benötigten Geräte wie z. B. Router, Switches, Firewalls, Netzwerkdienstserver, etc. Diese LAN-Interconnect Services bauen eine direkte, sichere und schnelle Verbindung, zwischen dem auswärtigen Überwachungszentrum des externen LEs und dem Netz des Parlamentes. Über diese Verbindungen werden die Dienstleistungen für die Überwachung, den Betrieb und die Wartung für alle Standorte erbracht. Diese Verbindungen wirken einer Gefährdung entgegnen und ermöglichen eine hohe Verfügbarkeit und somit einen hochwertigen Service.

Die EFK ist der Ansicht, dass die Sicherheit durch die Anwendung von Standards und Normen hoch ist und sich positiv auf die Wartung und Betrieb auswirken.

4.2 Die Verwaltung der Benutzer und Geräte im Parlament ist geregelt

4.2.1 Die Verantwortlichkeiten zwischen Parlament und Parlamentsdiensten sind geregelt

Das vom GS erlassene Dokument «Governance der Informationssysteme der Bundesversammlung» definiert den Rahmen für die Führung und Entwicklungssteuerung, Projektmanagement, Releasemanagement, IKT-Controlling, Risikomanagement, Informatikbetrieb und die Zuständigkeiten. Die Verwaltungsdelegation hatte im Rahmen der Budgetdebatte 2012 für die folgende Legislatur Service Pakete für die Ratsmitglieder definiert, welche dem DINT zur Umsetzung in Auftrag gegeben wurden. Mit den Leitplanken «Standardisierung» und «Wirtschaftlichkeit» hat der DINT ein Kommunikationspaket und ein Endgeräteangebot ausgearbeitet. Das Angebot wurde durch die Verwaltungsdelegation anerkannt. Sie hat entsprechende Weisungen zur Nutzung durch die Parlamentarier erlassen. Der DINT ist für die technische und organisatorische Umsetzung dieser Dienstleistungen verantwortlich.

Jedes Ratsmitglied kann ein Kommunikationspaket wählen. Er hat weiter die Wahl zwischen eigenen Endgeräten mit/ohne Zertifikat des Parlamentsdienstes oder einem Gerät des Parlamentsdienstes. Letzteres ist ein sicherheitstechnisch gehärtetes, vom DINT verwaltetes Endgerät, d. h. Sicherheitsrelevante Einstellungen und Software werden zentral vom DINT verwaltet und automatisch aktualisiert, sobald das Gerät am Netz angemeldet wird.

---

[3] ISO/IEC 27000 ist eine Reihe von Standards der IT-Sicherheit. Herausgegeben werden die über 20 Normen (Stand: Juni 2013) von der International Organization for Standardization (ISO).

[4] IT Infrastructure Library (ITIL) ist eine Sammlung von Best Practices in einer Reihe von Publikationen zur Umsetzung eines IT-Service-Managements (ITSM)

Die EFK ist allerdings der Auffassung, dass die Weisungen der Verwaltungsdelegation aktualisiert werden sollten. In der «Datenkommunikations-Dienstleistungen für die Ratsmitglieder der 49. Legislatur (2013-2015)» wird zum Beispiel nur auf ein Notebook verwiesen, ohne generell mobile Endgeräte zu regeln.

Ein Rückblick auf die verschiedenen Vorkommnisse bei den Parlamentariern bei der Nutzung von Mobilen Geräten zeigt, dass einerseits ein gehärtetes Endgerät, wie es z. B. der DINT anbietet und andererseits ein adäquates Verhalten des Benutzers einen Cyberangriff zumindest erschweren. Die Verwaltungsdelegation sollte in ihren Weisungen auf die Sorgfaltspflicht hinsichtlich Schutz der IKT hinweisen und regelmässig das Bewusstsein für den Umgang mit persönlichen und klassierten Informationen fördern.

4.2.2 Der sicherheitstechnische Zustand der Geräte wird aktiv überwacht

Die vom DINT abgegebenen Geräte sind sicherheitstechnisch gehärtet und werden, sobald sie am Netz des Parlaments sind, geprüft und aktualisiert. Die Systemadministratoren können, basierend auf einer Geräte-Datenbank, die Aktualität der Konfiguration der abgegebenen Geräte aktiv überwachen. Sie können feststellen, ob ein Gerät schon länger nicht mehr am Netz war und nicht aktualisiert wurde. In der Folge steht ihnen die Möglichkeit zur Verfügung, den Benutzer zu kontaktieren.

Während den Sessionen bietet der DINT im Parlamentsgebäude einen Beratungsstand (Security-Tankstelle) an. Wer interessiert ist, kann seine Geräte einem Gesundheitscheck unterziehen. Das Resultat wird jeweils schriftlich abgegeben. Wenn gewünscht kann auch eine persönliche Beratung genutzt werden.

Die EFK ist der Ansicht, dass die angebotenen Leistungen den erwarteten Sicherheitsstandards entsprechen. Die aufgestellte «Security-Tankstelle» bietet dem interessierten Benutzer die Möglichkeit sich zu informieren, unabhängig davon, ob er sein eigenes Gerät oder eines des DINT benutzt.

4.2.3 Die Zugriffsrechte werden regelmässig kontrolliert

Wie vorstehend erläutert unterscheidet der DINT drei Kategorien von Geräten. Mittels eines eingesetzten Verwaltungstools wird den Geräten, basierend auf den eingebauten Zertifikaten, Zugang zu den verschiedenen Netzen erlaubt bzw. entzogen. Ebenso werden die Benutzer-Berechtigungen über das Tool aktiviert oder deaktiviert. Die Benutzerrechte der Mitarbeitenden der Parlamentsdienste werden mindestens einmal jährlich anhand einer durch den Vorgesetzten zu bestätigenden Liste verifiziert. Zeitlich beschränkte Benutzerkonten werden spätestens vor Ablauf beim Administrator aufgelistet. Wird nichts unternommen, wird das Konto automatisch gesperrt.

Die EFK ist der Auffassung, dass mit der vorliegenden Lösung mit geringem Verwaltungsaufwand eine zuverlässige Ressourcenverwaltung und Zugangssteuerung möglich ist.

4.3 Das Netzwerk wird professionell überwacht und gewartet

4.3.1 Kontinuierliche Überwachung des Betriebes und der Sicherheit

Während das NOC des externen LEs die Netzwerk Architektur bezüglich optimalem Betrieb überwacht, widmet sich ein professionelles, zertifiziertes Security Operation Center (SOC) 7x24h den Netzwerkzonen und Firewalls. Schutz vor typischen Cyber Attacks ist auf verschiedenen Stufen vorhanden. Der externe LE überwacht die Netzwerkinfrastruktur auch auf aussergewöhnliche Aktivitäten.

Der Bereich Betrieb des DINT wird mit Rückmeldungen über den Gesundheitszustand und festgestellte Engpässe oder Vorfälle vom externen LE informiert. Er hat Zugang zum Live Inventar der Netzwerkverbindungen.

Mit dem eingesetzten Managementtool kann der Sicherheitsverantwortliche (ISBD) im DINT nebst den Rückmeldungen des externen LE und den regelmässigen Rapports auch eigene Analysen auslösen. Er hat Zugriff auf alle Informationen zu Ereignissen im Netzwerk.

Die EFK ist der Auffassung, dass die aktuelle Organisation mit Cyberrisiken umgehen kann. Unzuverlässige Geräte werden automatisch in eine separate Zone mit eingeschränkten Möglichkeiten geleitet. Eindringlinge müssen mehrere Hürden überwinden. Alle Netzwerkkomponenten werden kontinuierlich überwacht. Der Informationsaustausch über die aktuelle Bedrohungslage ist da. Es konnte nicht festgestellt werden, dass der Wechsel zu einem externen LE die Situation negativ beeinflusst hat.

4.3.2 Adäquates Change Management und Controlling

Über das Change Management werden neue Anforderungen umgesetzt sowie Verbesserungen von Engpässen vorgenommen, welche man aus der Betriebsüberwachung erkannt hat. Dazu trifft sich der Kundenbetreuer des externen LEs und Verantwortliche des BIT unter der Führung des DINT einmal jährlich. In diesem Gespräch werden die erkannten Situationen, situationsabhängig unter Beizung entsprechender Fachpersonen, mit Massnahmen ergänzt und umgesetzt.

Bei den Verträgen liegen umfangreiche Subverträge vor. Gemäss eigenen Aussagen wurde die Ablage erst kürzlich umstrukturiert. Ob das Controlling der geleisteten und zu bezahlenden Leistungen funktioniert, wurde von der EKF in diesem Prüfauftrag nicht untersucht.

Das Outtasking bringt aus Sicht der EFK Vorteile bei der Ausstattung des Netzwerkes durch eine performante und skalierbare Lösung. Es besteht ein hohes Niveau in Bezug auf Sicherheit durch die 7x24h Überwachung und durch das umfangreiche Reporting. Nachteilig fallen die höheren Betriebs- und Unterhaltskosten auf. Diese werden jedoch durch die grössere Funktionalität wieder relativiert.

5 Diverses – Abklärungen bei einzelnen Buchungen

Anlässlich unserer Prüfung ergaben sich einige Fragen betreffend Buchungen in den Informatikkonten 3114001000 – 311450100, insbesondere bezüglich Mehrfachbuchungen und Stornierungen. Die entsprechenden Fragen der EFK konnten an der Schlussbesprechung mit ergänzenden Auskünften der Parlamentsdienste zufriedenstellend geklärt werden.

6 Follow up der PA 11324 und 11461

6.1 PA 11324 «Finanzielle Führung Beschaffungswesen und Informatik»

Empfehlung 3.2 (Priorität 1)

Die EFK empfiehlt der Geschäftsleitung und der Verwaltungsdelegation die Berichterstattung über die finanzielle Führung der Parlamentsdienste (inkl. einem modernen auf die Verwaltung abgestimmten Controlling-Konzept) auszubauen. Zur Unterstützung und Verbesserung der Transparenz und Abbildung von Prozessen und Abläufen wäre ein Managementinformations-system sehr hilfreich.

Die Parlamentsdienste haben ein Monatsreporting über den Stand der Kredite eingeführt. Das Reporting wurde erstmals per Juli 2014 erstellt und an die Geschäftsleitung wie auch an die Verwaltungsdelegation abgegeben. Zudem wurde auch ein monatliches Reporting mit Forecast über die IKT-Kredite der Kostenstellen 3163 DINT und 3173 DINT-Investitionen eingeführt. Der Forecast ermittelt die Abteilung DINT und liefert die Daten auf der vom Finanzdienst zur Verfügung gestellten Excel-Tabelle. Ein Controlling-Konzept konnte der EFK nicht vorgelegt werden, jedoch wird im Rahmen der Umsetzung der Strategie der PD 2012 – 2016 das Projekt «Transparences des coûts» (ein Kennzahlensystem) eingeführt.

Die Parlamentsdienste verzichteten auf ein Managementinformationssystem. Die Dokumente werden zurzeit im Tool «DokVerwaltung» abgelegt. Es ist vorgesehen, dass die gesamte Bundesverwaltung bis spätestens zum Jahr 2022 ein Dokumentenverwaltungssystem einführt. Die Parlamentsdienste prüfen dann, ob diese Applikation übernommen wird.

Die Empfehlung 3.2 wurde umgesetzt.

Empfehlung 3.3 (Priorität 1)

Die EFK empfiehlt der Geschäftsleitung des Parlamentsdienstes, das Interne Kontrollsystem zu verbessern, indem

- *eine für das IKS verantwortliche Person bestimmt wird, die nicht zugleich die Funktion des Leiters Finanz- und Reisedienst inne hat;*
- *die Weisungen, die Unterschriftenregelung (inkl. Visalisten) und die Formulare von Zeit zu Zeit auf ihre Aktualität hin überprüft werden;*
- *die Risiko-Kontroll-Matrixen mit den durchzuführenden IKS-Kontrollen ergänzt werden;*
- *die Unterschriftenregelung auf den Rechnungen geprüft und eingehalten wird*

Bei den IKS-Prüfungen im Bereich der Beschaffungen hat die EFK festgestellt, dass ein Riskmanagement (RM) mit Massnahmen erstellt worden ist. Jedoch besteht noch kein entsprechendes IKS, die die Risiken im Riskmanagement mit entsprechenden Kontrollen überprüft und bei Fehler wie Doppelzahlungen, unkorrekte Buchungen (Spezifikation, systematische Buchungsfehler) korrigierend eingreift. Eine Arbeitsgruppe RM/IKS ist vorhanden. Der letzte Workshop fand am 27. August 2012 statt. Im Bereich des RM finden regelmässige Sitzungen statt.

Die Empfehlung 3.3 «das Interne Kontrollsystem ist zu verbessern», wurde bis zum heutigen Zeitpunkt aus dem Blickwinkel Beschaffung noch nicht zufriedenstellend umgesetzt.

Empfehlung 6. 2 (Priorität 1)

Die EFK empfiehlt der Geschäftsleitung der Parlamentsdienste eine zentrale Beschaffungsstelle mit einem Vertragsmanagement-Tool einzuführen. Parallel dazu sind die Dossierstrukturen und die Ablage der Unterlagen (Aufbewahrungsdauer mindestens 3 Jahre nach Abschluss des Vertrages) zu regeln.

Die PD haben einen Support für die Beschaffungs-Beteiligten eingeführt. Auch das Vertragsmanagement Bund soll ab Januar 2015 operativ sein. Dossier Strukturen wurden eingeführt und die Aufbewahrungsdauer geregelt.

Zu der Umsetzung dieser Empfehlungen äussert sich die EFK im Rahmen dieses Berichtes.

Die Empfehlung 6.2 kann somit als umgesetzt betrachtet werden.

Empfehlung 6.3 (Priorität 1)

Die EFK empfiehlt der Geschäftsleitung zur Steigerung der Qualität und Transparenz im Beschaffungsprozess u. a. Folgendes: Die für das Vertragswesen zuständigen Mitarbeiter und Mitarbeiterinnen sind im öffentlichen Beschaffungs-/Vertragswesen aus- bzw. weiterzubilden. Es ist mehr Wettbewerb zu schaffen; der Grundsatz des freien Wettbewerbs ist einzuhalten. Zur Verbesserung des Beschaffungsprozesses sind inskünftig Laufzettel und Checklisten (Beschreibung des Vorgehens, Visa usw.) zu verwenden.

Die Schulung der Ansprechperson für die Beschaffungs-Beteiligten erfolgte. Weitere zuständige Mitarbeiter wurden sensibilisiert. Es wurde auch vermehrt Wettbewerb geschaffen sowie Laufzettel und Checklisten eingeführt.

Zu der Umsetzung dieser Empfehlungen äussert sich die EFK im Rahmen dieses Berichtes.

Die Empfehlung 6.3 kann somit als umgesetzt betrachtet werden.

Empfehlung 8.6.1 (Priorität 2)

Die EFK empfiehlt der Geschäftsleitung zur Steigerung der IT-Sicherheit:

- *Das IT-Sicherheitsmanagement der PD sollte nach den allgemein gültigen und anerkannten Standards von ISO 27000/n aufgebaut werden.*
- *Eine IT-Security Policy sollte erstellt und durch die Verwaltungsdelegation verabschiedet werden.*
- *In einem IT-Sicherheitskonzept sollten sodann die Grundsätze und die Prozesse zur Erreichung einer angemessenen Sicherheit festgelegt werden.*

Ein Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27001 wurde eingeführt. Zusammen mit den Sicherheitsüberwachungen und Hinweisen des externen Leistungserbringers können sowohl automatische, wie auch gezielte Sicherheitsanalysen durchgeführt werden.

Eine IT-Security Policy für Parlamentarier konnte nicht durchgesetzt werden. Es wurden jedoch Massnahmen zur Separation auf Ebene der Netzwerkzugänge getroffen. Sicherheitskonzepte gibt es auf der Netzwerkebene und im Bereich der Netzwerkzugänge. Zum Sicherheitskonzept äussert sich die EFK im Bericht.

Die Empfehlung 8.6.1 kann als umgesetzt betrachtet werden.

Empfehlung 8.6.2 (Priorität 2)

Damit eine minimale «Gesundheit» aller Endgeräte sichergestellt werden kann, sollte eine Sicherheitszertifizierung (mit Label) durch DINT für alle Geräte eingeführt werden.

Periodisch unternehmen die DINT Awareness-Aktionen bei den Räten vor Ort. Diese « Security-Tankstelle» können die Parlamentarier freiwillig aufsuchen. Sie können ihre Geräte durchchecken lassen und erhalten ein Zertifikat mit den entsprechenden Angaben zum Gesundheitszustand ihres Gerätes. Sie erhalten auf Wunsch ebenfalls Hinweise und Beratung zur Erhöhung ihres Schutzes bezüglich Cyber-Risiken.

Die Empfehlung 8.6.2 wurde umgesetzt.

6.2 PA 11461 «Überprüfung der IT Sicherheit bei den Parlamentsdiensten»

Empfehlung 4.1a_1 (Priorität 2)

Es sollte ein Prozess definiert werden, damit die AD-Domain mit allen Accounts regelmässig und systematisch überprüft wird. Die bestehenden Unregelmässigkeiten sollten rasch abgeklärt werden.

Es wurde ein Identitiy Managementsystem (ein AÜM – Automated User Management) und die periodische Überprüfung der auf den Systemen vorhandenen Nutzer durch die Vorgesetzten eingeführt.

Die Empfehlung 4.1a_1 wurde umgesetzt.

Empfehlung 4.1a_2 (Priorität 1)

In der Active Directory sind keine eindeutigen Namen für alle Account-Typen festgelegt, obschon solche Konventionen im Bundesumfeld bestehen. Normalerweise wird in dem AD ein «unique-key» (z. B. die Personalnummer) verwendet und dieser mit einem Präfix versehen. Heute ist bei den PD die Kontrolle der Accounts sehr schwierig, weil diese nur teilweise korrekt anhand des Namens identifiziert werden können. Die EFK empfiehlt daher eine einheitliche Namenskonvention einzuführen und diese bei den Ratsmitgliedern im Rahmen der bevorstehenden National- bzw. Ständeratswahlen umzusetzen.

Die Empfehlung 4.1a_2 wurde umgesetzt.

Empfehlung 4.1b_1 (Priorität 1)

Das Patchmanagement sollte auch für die vorhandenen UNIX- bzw. LINUX-Systeme schriftlich geregelt und mittels definiertem und kontrolliertem Prozess periodisch durchgeführt werden, um allfällig bestehende Risiken mit diesen Systemen zu eliminieren.

Ein Unix Distributionsserver wurde eingeführt und in Betrieb genommen.

Die Empfehlung 4.1b_1 kann als umgesetzt betrachtet werden.

Empfehlung 4.1b_2 (Priorität 2)

Der Einsatz des Microsoft-Werkzeugs «System Center Configuration Manager» (SCCM) ist zu prüfen und je nach Software-Konfiguration damit auch Updates von Non-Microsoft-Produkten (z. B. UNIX- und LINUX-Systeme) zu automatisieren.

Die Empfehlung wurde durch die Softwareverteilservices (Windows) und einer Softwaredistribution Plattform (Unix-Plattformen) umgesetzt. Sie wird durch die Standardisierung der Gerätepalette unterstützt.

Die Empfehlung 4.1b_2 ist umgesetzt.

7 Schlussbesprechung

Die Schlussbesprechung fand am 23. Oktober 2014 statt. Teilgenommen haben von den Parlamentsdiensten , , und und von der EFK die Herren Grégoire Demaurex, Peter Zumbühl, Stefan Wagner und Hans-Rudolf Michel.

Sie ergab grundsätzlich Übereinstimmung mit dem Inhalt des Berichtes. Die Bemerkungen der Parlamentsdienste wurden aufgenommen und sind weitgehend in den Bericht eingeflossen.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung den Amtsleitungen bzw. den Generalsekretariaten obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

Grégoire Demaurex	Peter Zumbühl
Mandatsleiter	Revisionsleiter

Anhang 1: Rechtsgrundlagen

Rechtsgrundlagen:

Finanzkontrollgesetz (FKG, SR 614.0)

Finanzhaushaltgesetz (FHG, SR 611.0)

Finanzhaushaltverordnung (FHV, SR 611.01)

Bundesinformatikverordnung (BinfV, SR 172.010.58)

Bundesgesetz über das öffentliche Beschaffungswesen (BöB, SR172.056.1)

Verordnung über das öffentliche Beschaffungswesen (VöB, SR 172.056.11)

Parlamentsverwaltungsverordnung (ParlVV, SR 171.115)

Anhang 2: Abkürzungen, Priorisierung der Empfehlungen der EFK

Abkürzungen:

BIT	Bundesamt für Informatik und Telekommunikation
DINT	Dienste für Informatik und Telekommunikation
EFK	Eidgenössische Finanzkontrolle
IKT	Informations- und Kommunikationstechnik
LE	Leistungserbringer
PARL	Bundesversammlung
PD	Parlamentsdienste
VD	Verwaltungsdelegation der eidgenössischen Räte
WTO	World Trade Organization

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. Dabei bezieht sich die Bewertung auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).