PRÜFBERICHT

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

Funktionsprüfung der Projekt-generierungs- und Kreditoren-prozesse in TDcost

ASTRA

27. August 2013

Das Wesentliche in Kürze

Das Bundesamt für Strassen (ASTRA) ist die Schweizer Fachbehörde für die Strasseninfrastruktur und den individuellen Strassenverkehr. Anfang 2008 trat die Neugestaltung des Finanzausgleichs und der Aufgabenverteilung zwischen Bund und Kantonen (NFA) in Kraft. Damit wurden Ausbau und Unterhalt der Nationalstrassen von den Kantonen an den Bund übertragen. Die Steuerung der Investitionskosten erfolgt beim ASTRA seit der Übernahme der Nationalstrassen über Projekte und nicht mehr über Budget- oder Teilkredite. Dieser Ansatz erforderte den Aufbau eines durchgängigen Systems, das das ASTRA von der Planung bis zur Abrechnung unterstützen sollte. Zur Erfüllung dieser Anforderungen führte das ASTRA im Jahre 2008 die Anwendung TDcost ein, die seit diesem Zeitpunkt laufend weiterentwickelt wird. TDcost ist ein Tool zur Verwaltung der Projektkosten (Kostenvoranschlag, Kredite, Verträge, Rechnungen und Garantien), zur Planung (Investitionsplanung, Meilenstein-Planung, Vergabeplanung) und zur Verwaltung des Jahresbudgets (Voranschlagskredite). Dadurch dient TDcost heute auch als Vorsystem der Finanzbuchhaltung des Bundes. Dabei werden jährlich über 22'000 Rechnungen in der Höhe von insgesamt mehr als 1,5 Milliarden Franken abgewickelt. Das eigentliche Zahlungs- und Buchhaltungssystem ist SAP.

Die Prüfung der EFK diente zur Beurteilung der Abwicklung der finanzrelevanten Geschäftsprozesse, der Güte des zugehörigen IKS sowie der Informatikaspekte von TDcost.

Die durchgeführte Prüfung zeigte verschiedene Risiken und Mängel auf, die zu entsprechenden Empfehlungen führten. Insbesondere ist festzuhalten, dass die Funktionentrennung im TDcost nicht zweckmässig ist und zu unvereinbaren Funktionskumulationen führt. Auf Grund der bestehenden Systemberechtigungen erscheint es durchaus als möglich, dass fiktive Rechnungen verbucht werden könnten und dass diese auch bezahlt würden. Es bestehen in diesem Bereich Kontrolllücken, die umgehend geschlossen werden müssen. Weitere identifizierte Kontrolllücken sind im Bericht aufgezeigt.

Die wesentlichen Investitionen in die Weiterentwicklung und den Ausbau der Anwendung von rund 4,2 Millionen Franken (im Vergleich zur Initialversion für Lizenzen von 1,6 Millionen Franken) machen aus dem ursprünglichen Standardprodukt TDcost eine Individualanwendung des ASTRA. Die Anwendung wird durch den Lieferanten (techdata) mit Hilfe eines Subunternehmers (TRIVADIS) gewartet und technisch betreut. Dies führt zu Abhängigkeiten vom Lieferanten wie auch vom Subunternehmer hinsichtlich personeller und auch technischer Aspekte. Diese Dreiecksbeziehung ist schon aus der Struktur heraus kostenintensiv und schränkt das ASTRA bei allfälligen Preisverhandlungen stark ein, da es für Weiterentwicklungen momentan gar keine Alternativen gibt. Zudem ist das Wissen über TDcost sowohl bei techdata als auch bei TRIVADIS auf wenige Personen verteilt. Ein Ausfall des Architekten von TDcost könnte das Ende für die Weiterentwicklung von TDcost bedeuten.

Die Firma techdata ist nicht nur Lieferant und Supporter von TDcost, sondern erbringt auch umfangreiche bautechnische Leistungen an das ASTRA. Da techdata in der Lage ist, die aktuellen Produktivdaten in TDcost (jedoch ohne die Details in FABASOFT) zu lesen, könnte sie sich gegebenenfalls einen Wissensvorsprung gegenüber den übrigen Anbietern verschaffen. Diese Situation darf aus Sicht der EFK nicht bestehen bleiben.

Im Weiteren wurde festgestellt, dass die Risiko-Kontrollmatrizen (RKM) wie auch die Dokumentation der durchgeführten Kontrollen die formellen Anforderungen an ein IKS nicht vollumfänglich erfüllen. Die RKM sollte mit den Ablaufdiagrammen im Führungssystem ASTRA abstimmbar sein und umgekehrt. Zudem ist das dokumentierte IKS in den Filialen gar nicht bekannt. Die Verbindung zwischen der RKM und den in der täglichen Arbeit durchzuführenden Kontrollen konnte nicht hergestellt werden, das IKS wird nicht gelebt. Die Existenz des IKS kann deshalb nur mit Einschränkungen bestätigt werden. Wenn die Überarbeitung der Dokumente vorgenommen wird, sollte auch geprüft werden, ob eine weitgehend verbindliche Standardisierung der Prozesse und Kontrollen in allen Filialen nicht effizienter wäre als die bisherige Heterogenität. Der administrative Aufwand könnte auf ein notwendiges Minimum beschränkt und Synergien besser genutzt werden.

Die EFK gelangte schliesslich zur Überzeugung, dass die Anwendung TDcost den Anforderungen an ein finanzrelevantes Vorsystems nicht genügt. Es wurde als Hilfsmittel für Projektleiter konzipiert und für das Baukostenmanagement des ASTRA ausgebaut. Die Abwicklung der Rechnungen erfordert jedoch die Qualitäten und Sicherheiten eines Finanzsystems. Die Anforderungen an die Datensicherheit, die Belegsicherheit, die Journalisierung und das interne Kontrollsystem (IKS) sind zu wenig ausgebaut. Zudem können wichtige Funktionen zur Unterstützung der Projektleiter und Filialen auf Grund der fehlenden Funktionalitäten nicht in TDcost vorgenommen werden. Es werden deshalb weiterhin verschiedene (manuelle) Excel-Tabellen eingesetzt. Damit die Ordnungsmässigkeit der Rechnungsbearbeitung sichergestellt werden kann, müsste TDcost zu einer umfassenden Anwendung im Sinne eines finanzrelevanten Vorsystems ausgebaut werden. Aufgrund der bereits bestehenden Probleme mit der Performance und der Komplexität der Applikation ist es fraglich, ob eine solche Lösung mit TDcost finanziell vertretbar bzw. nachhaltig ist. Eine Konzentration des gesamten Wissens über TDcost als unverzichtbare Anwendung beim ASTRA auf einige wenige Personen wird als sehr grosses Risiko eingestuft. Daher sollten auch Alternativen betrachtet werden: Entweder ist der Kreditorenprozess aus TDcost herauszulösen und mit einer entsprechenden Anwendung zu bearbeiten oder eine mittelfristige Ablösung von TDcost sollte vorbereitet werden.

Die Empfehlungen der EFK werden vom ASTRA aufgenommen und entsprechende Massnahmen sind in die Wege geleitet. In diesem Bericht sind die vom Amt vorgesehenen Massnahmen jeweils bei den Empfehlungen, grau hinterlegt, als Stellungnahme integriert. Mit der Medienmitteilung vom 4. November 2013 hat das ASTRA zudem mitgeteilt, dass es ein Evaluationsverfahren für die Ablösung von TDcost starten will.

Generelle Stellungnahme des ASTRA zur Revision:
Nach Ansicht des Bundesamts für Strassen ASTRA erfüllt das Instrument TDcost heute seinen Zweck und erlaubt es, das investive Nationalstrassengeschäft mit vertretbaren Risiken zu führen. Dies bedeutet jedoch nicht, dass das ASTRA die Empfehlungen der EFK nicht nachvollziehen kann; insbesondere mittel- und langfristig zeichnen sich unbestreitbar Herausforderungen ab. Das ASTRA wird daher die Hauptempfehlung umsetzen und die Anwendung TDcost ablösen. Es handelt sich dabei um ein mittelfristiges Vorhaben im hohen Risikobereich, was Kosten, Termine, Inhalte und auch Reputation anbelangt. Dennoch ist das ASTRA überzeugt, mit diesem Entscheid langfristig die Risikosituation in seinem Kreditorenprozess positiv beeinflussen zu können. Kurzfristig wird das ASTRA mittels Verbesserungen der Anwendung und Anpassung der Abläufe die erkannten Schwachpunkte eliminieren. Die detaillierte Stellungnahme des ASTRA zu den einzelnen Empfehlungen wurde der EFK zugestellt.

Auf genereller Ebene legt das ASTRA Wert auf folgende Feststellungen:

TDcost ist einerseits das zentrale Instrument der Abteilung Strasseninfrastruktur für das Projekt- und Projektportfoliomanagement und andererseits ein Vorsystem für die Finanzbuchhaltung des Bundes. Die Anwendung deckt also die Bedürfnisse zweier völlig unterschiedlicher Anspruchsgruppen ab:

70 Projektleiter an acht Standorten und in drei Sprachen benutzen TDcost, um die Kosten, Termine und Inhalte von gegenwärtig ca. 800 Projekten mit über 10'000 Verträgen im Griff zu behalten. Für die Hierarchie vom Chefprojektleiter bis zum Amtsdirektor ist zudem von grosser Bedeutung, dass auch das Projektportfolio mit dieser Anwendung bewirtschaftet werden kann. Ein verlässlicher Budgetierungs- und Finanzplanungsprozess wäre ohne die Informationen aus TDcost nicht möglich.

Auf der anderen Seite ist TDcost ein Arbeitsinstrument für das operative Investitionscontrolling und dient als Vorsystem für die Finanzbuchhaltung des Bundes. Dank TDcost kann die Abteilung Strasseninfrastruktur jährlich zwischen 20'000 und 30'000 Rechnungen in den vorgegebenen Fristen (zu 98%), an die richtigen Empfänger, in den richtigen Beträgen und unter Einhaltung der freigegebenen Kredite bearbeiten und bezahlen.

Die Prüfung der EFK konzentrierte sich auf die zweite Funktion, den Kreditorenprozess. Die andere Hälfte der Anforderungen, das Projekt- und Portfoliomanagement, war nicht Gegenstand der Prüfung. Eine umfassende und abschliessende Beurteilung der Anwendung TDcost ist auf der Basis des vorliegenden Berichts nach Ansicht des ASTRA nicht möglich.

L'essentiel en bref

L'Office fédéral des routes (OFROU) est l'autorité suisse compétente en matière d'infrastructure routière et du transport routier individuel. La réforme de la péréquation financière et de la répartition des tâches entre la Confédération et les cantons (RPT) est entrée en vigueur au début de l'année 2008. Ainsi, l'expansion et l'entretien des routes nationales ont été transférées des cantons à la Confédération. Depuis la reprise des routes nationales, l'OFROU contrôle les coûts d'investissement par le biais de projets et non plus au moyen de crédits budgétaires ou de crédits partiels. Afin de répondre à ces exigences, il avait donc besoin d'un système uniformisé qui pouvait l'aider de la planification au décompte final. L'OFROU a introduit en 2008 l'application TDcost qui est en constante évolution depuis lors. TDcost est un outil destiné à la gestion des coûts de projets (devis, crédits, contrats, factures et garanties), à la planification (investissements, échéances, adjudications) et à l'administration du budget annuel (crédits budgétaires). Ainsi, TDcost sert aujourd'hui de système auxiliaire à la comptabilité financière de la Confédération. Chaque année, plus de 22 000 factures d'un montant total supérieur à 1,5 milliard de francs sont traitées. SAP sert système de paiement et de système de comptabilité.

L'audit du CDF a permis d'évaluer l'exécution des processus qui ont une incidence financière, la qualité du système de contrôle interne (SCI) et les aspects informatiques de TDcost.

L'audit a montré différents risques et lacunes qui ont conduit le Contrôle fédéral des finances à formuler des recommandations. Il convient en particulier de signaler que la séparation des fonctions dans TDcost n'est pas adéquate et qu'elle mène à des cumuls de fonctions incompatibles. En raison des autorisations d'accès existantes dans le système, il est tout à fait possible que des factures fictives soient comptabilisées et payées. Les lacunes au niveau du contrôle dans ce domaine doivent être comblées sans délai. Le rapport fait en outre état d'autres insuffisances à ce niveau.

Les importants investissements de 4,2 millions de francs pour le développement et l'extension de l'application (en comparaison, la version initiale avec les licences avait coûté 1,6 million de francs) font à présent du produit standard d'origine TDcost une application individuelle de l'OFROU. La maintenance et l'assistance technique de l'application sont assurées par le fournisseur (techdata) avec l'aide d'un sous-traitant (TRIVADIS). L'OFROU devient ainsi dépendant du fournisseur et du sous-traitant en ce qui concerne les aspects humains et techniques. Outre les coûts élevés de cette relation triangulaire, la marge de manœuvre de l'OFROU est extrêmement faible lors de négociations de prix, car il n'y a pour le moment pas d'autre solution de développement pour une telle application. De plus, peu de personnes maîtrisent TDcost chez techdata et chez TRIVADIS. En d'autres termes, le développement de l'application pourrait prendre fin avec une défection de l'architecte de TDcost.

La société techdata n'est pas seulement le fournisseur et le responsable de l'assistance de TDcost, mais elle accomplit également des prestations architecturales de grande envergure pour l'OFROU. Comme techdata est en mesure de lire les dernières données de production dans TDcost (sans toutefois avoir accès aux détails dans FABASOFT), elle pourrait acquérir, le cas échéant, une longueur d'avance sur les autres fournisseurs. Le CDF estime que cette situation ne peut pas subsister.

De plus, il a été constaté que la matrice de contrôle des risques ainsi que la documentation des contrôles effectués ne remplissent pas entièrement les exigences formelles attendues d'un système de contrôle interne. La matrice de contrôle des risques devrait pouvoir être adaptée aux diagrammes de flux du système de gestion de l'OFROU et inversement. En outre, les filiales de l'OFROU n'ont pas connaissance du SCI documenté. Le lien entre la matrice de contrôle des risques et les contrôles à effectuer au quotidien n'a pas pu être établi car le SCI n'est pas vécu. Ainsi, l'existence du SCI ne peut être confirmée que partiellement. Si la révision du document est faite, il faudrait également examiner si la standardisation des processus et des contrôles dans toutes les filiales ne serait pas plus efficace que l'hétérogénéité qui existe actuellement en la matière. Les charges administratives pourraient être limitées au strict nécessaire et les synergies mieux exploitées.

Le CDF est finalement parvenu à la conviction que TDcost ne répond pas aux exigences posées à un système comptable auxiliaire pertinent. TDcost a été conçu comme instrument d'aide pour les responsables de projets et développé pour la gestion des coûts de construction de l'OFROU. Le traitement des factures exige toutefois la qualité et la sécurité offertes par un système financier. Les exigences liées à la sécurité des données, à la journalisation, à la sécurité des justificatifs comptables et au système de contrôle interne sont insuffisantes. De plus, en raison de l'absence des fonctionnalités nécessaires dans TDcost, il est impossible de proposer aux responsables de projets et aux filiales diverses fonctions qui pourraient leur être d'une grande aide. Pour le moment, différents tableaux manuels en format Excel sont prévus à cet effet. Afin que la régularité du traitement des factures soit assurée, TDcost devrait être développé comme un système financier auxiliaire à part entière. En raison des problèmes de performance existants et de la complexité de l'application, il y a lieu de se demander si une telle solution avec TDcost est financièrement acceptable et durable. De plus, le fait que la connaissance globale de cette application indispensable à l'OFROU repose sur quelques personnes représente un risque très élevé. C'est pourquoi il faut considérer d'autres possibilités. Il faut soit extraire les processus fournisseurs de TDcost et les traiter avec une application adéquate, soit préparer un remplacement à moyen de terme de TDcost.

L'OFROU accepte les recommandations du CDF et entreprend les mesures nécessaires. Dans le rapport, les mesures prévues par l'office sont jointes sous la forme de prises de position aux recommandations, surlignées en gris. Dans un communiqué de presse daté du 4 novembre 2013, l'OFROU a indiqué vouloir débuter une procédure d'évaluation pour remplacer TDcost.

Inhaltsverzeichnis

1 Auftrag und Vorgehen

1.1 Ausgangslage

Das Bundesamt für Strassen (ASTRA) ist die Schweizer Fachbehörde für die Strasseninfrastruktur und den individuellen Strassenverkehr. Anfang 2008 trat die Neugestaltung des Finanzausgleichs und der Aufgabenverteilung zwischen Bund und Kantonen (NFA) in Kraft. Damit wurden Ausbau und Unterhalt der Nationalstrassen von den Kantonen an den Bund übertragen. Die Steuerung der Investitionskosten erfolgt beim ASTRA seit der Übernahme der Nationalstrassen über Projekte und nicht mehr über Budget- oder Teilkredite. Dieser Ansatz erforderte den Aufbau eines durchgängigen Systems, das das ASTRA von der Planung bis zur Abrechnung unterstützen sollte. Zur Erfüllung dieser Anforderungen führte das ASTRA im Jahre 2008 die Anwendung TDcost ein, die seit diesem Zeitpunkt laufend weiterentwickelt wird. TDcost ist ein Tool zur Verwaltung der Projektkosten (Kostenvoranschlag, Kredite, Verträge, Rechnungen und Garantien), zur Planung (Investitionsplanung, Meilenstein-Planung, Vergabeplanung) und zur Verwaltung des Jahresbudgets (Voranschlagskredite). Dadurch dient TDcost heute auch als Vorsystem der Finanzbuchhaltung des Bundes.

Die Anwendung TDcost wird als Vorsystem von SAP eingesetzt und dient der Planung der Kredite und der Abwicklung der Rechnungen für die Projekte der Nationalstrassen. Die Projekte betreffen Ausbau, Unterhalt, Betrieb sowie die Engpassbeseitigung von Nationalstrassen. Dabei werden jährlich mehr als 1.5 Milliarden Franken (inkl. Kosten für den Betrieb der Nationalstrassen) ausbezahlt. Nach Angaben des ASTRA erfolgten in den letzten Jahren bloss eine Handvoll falsch ausgeführter Zahlungen, welche aber alle vollumfänglich zurückbezahlt wurden.

Die Funktionalitäten von TDcost unterstützen unter Anderem folgende Geschäftsprozessschritte der Projekte:

- Erfassen der Projektstammdaten, der Projektstruktur und der Kostenvoranschläge (KV)
- Kostenvoranschläge in Form eines Gesamtkredites erfassen und freigegeben
- Verträge und Voranschlagskredite (welche der jährlichen Tranche des Gesamtkredites entsprechen) erfassen und freigegeben
- Die Rechnungen erfassen, Schwellen prüfen, Rechnungen genehmigen und nach der Freigabe durch die Zentrale zum Bezahlen an SAP weiterleiten.

Die bisherigen Prüfungen bezogen sich auf den Jahresabschluss und auf die Schnittstelle zwischen TDcost und SAP. Die Prüfung diente einerseits dazu eine umfassende Sicht der Applikation zu erhalten und andererseits wurde die Abwicklung der finanzrelevanten Geschäftsprozesse beurteilt.

1.2 Prüfungsziel und –fragen

Die Prüfziele waren die Beurteilung des Betriebs von TDcost bezüglich Sicherheit und Verfügbarkeit, sowie die Beurteilung der Wirksamkeit des internen Kontrollsystems (IKS) bei den in TDcost abgewickelten Prozessen.

Der Auftrag enthielt Fragen zu den finanzrelevanten Prozessen, die mit TDcost abgewickelt werden und zum internen Kontrollsystem. Dabei wurden die beiden Prozesse *Projektgenerierung* und *Kreditorenprozess* zur Prüfung ausgewählt. In diesen Prozessen wurden die verwendeten Projektstrukturen und Abläufe, sowie die Wirksamkeit des IKS beurteilt.

Ein weiterer Themenkomplex betraf den Betrieb der Anwendung TDcost. Dabei standen Fragen zu Verfügbarkeiten, der Betriebssicherheit, den SLA, den Abhängigkeiten (von Fachspezialisten und Lieferanten), zur Entwicklung und zum Change Management sowie zum technischen Support im Zentrum.

Weitere Informatikthemen waren die Schnittstellen zwischen TDcost sowie den vor- und nachgelagerten Systemen und die Umsetzung der Zugriffs- und Sicherheitskonzepte.

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Herrn Peter Bürki als Revisionsleiter im Team mit Frau Carole Balli sowie den Herren Daniel Zoss, Hans-Jörg Uwer und Stéphane Kury durchgeführt. Die Themen wurden sowohl im Bereich Investitionscontrolling der Zentrale (IC), wie auch im Bereich IC der Filialen Winterthur, Estavayer-le-Lac und Bellinzona geprüft. Im technischen Bereich wurde zudem ein Interview mit der Firma *techdata* (Lizenzgeber von TDcost) zu Fragen rund um TDcost geführt.

Neben den anwendungsorientierten IT-Prüfungen wurden die generellen IT-Kontrollen (ITGC) nach dem Prüfungsstandard PS 890 in der Zentrale und reduziert in den besuchten Filialen geprüft. Die ITGC der Leistungen des BIT werden separat geprüft. Diese Prüfung ist zurzeit in Arbeit. Die Informationen, die TDcost betreffen, werden dem ASTRA zur Verfügung gestellt.

Die Prüfung des Internen Kontrollsystems erfolgte nach den Schweizer Prüfungsstandards und richtete sich nach dem „Vorgehensmodell Anwendungsprüfung“ der Treuhandkammer vom 20. Mai 2008.

Die Schlussfolgerungen im Bericht stützen sich auf stichprobenweise Prüfungen von Belegen und Transaktionen sowie zahlreiche Interviews. Die Festlegung dieser Stichproben basiert auf dem Prinzip der Wesentlichkeit und auf Risikoüberlegungen zu den in die Prüfung einbezogenen Bereichen der Geschäftstätigkeit. Es handelt sich also nicht in allen Fällen um repräsentative Stichproben.

Bei der Beurteilung der einzelnen Teilprozesse werden, bezogen auf die Risiken der festgestellten Kontrolldefizite für wesentliche falsche Angaben in der Jahresrechnung, die folgenden Symbole verwendet:

▲ Es liegt ein bedeutender Mangel vor. Für die Verwaltungseinheit besteht dringender Handlungsbedarf. Es gibt keine oder praktisch keine internen Kontrollen. Das IKS ist unzuverlässig. Die Existenz kann deshalb für diesen Prozess nicht bestätigt werden.

■ Es besteht ein bedeutendes Verbesserungspotenzial, das von der Verwaltungseinheit umgesetzt werden muss. Es gibt zwar oftmals Kontrollen, diese sind aber nicht standardisiert und / oder stark von einzelnen Personen abhängig. Das IKS findet sich lediglich auf einer informellen Ebene. Die Existenz kann für diesen Prozess nur mit Einschränkung bejaht werden.

● Die Ergebnisse entsprechen den Erwartungen der EFK. Es besteht kein oder lediglich ein geringfügiges Verbesserungspotenzial. Die Existenz des IKS wird für diesen Prozess bestätigt.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte erfolgten zuvorkommend und kompetent. Die Gesprächspartner in den Filialen und die Büroräumlichkeiten standen jeweils zeitgerecht zur Verfügung. Die gewünschten Unterlagen wurden der EFK übergeben bzw. konnten eingesehen werden. Die benötigte Infrastruktur und das Q-System von TDcost standen für die Prüfungen der Anwendung zur Verfügung.

2 Der generelle Aufbau des IKS im ASTRA

2.1 Risikomanagement Konzept ist definiert

Für das Risikomanagement hat das ASTRA ein Konzept definiert, das im Führungssystem ASTRA (FS ASTRA) abgebildet ist. Die Risikoerhebung erfolgt für das strategische Risikomanagement mittels eines „top-down“ Ansatzes, das operative Risikomanagement mittels eines „bottom-up“ Ansatzes. Für die Risikoerhebung findet jährlich ein Risikoassessment mittels einer Szenario-Analyse statt. Der Metaprozess – Risiken identifizieren, Risiken bewerten, Risiken steuern sowie Risiken überwachen und berichten – ist standardisiert.

Zur einheitlichen Erfassung der Risiken und Chancen liegen standardisierte Unterlagen vor, die eine wesentliche Unterstützung in den zuständigen Bereichen bringen sollen. Das Konzept gibt dem Nutzer ein detailliertes und nachvollziehbares Fachdokument, das es ermöglicht sowohl die strategischen als auch die operativen Risiken aufzunehmen und zu beurteilen. Die unterstützenden Hilfsmittel stellen sicher, dass auf Amtsstufe eine einheitliche Vorgehensweise sichergestellt wird. In der generischen Risikosteuerung wird kurz auf das Interne Kontrollsystem hingewiesen, Verbindungen zwischen den identifizierten Risiken und dem implementierten internen Kontrollsystem fehlen. Es sollte nachweisbar sichergestellt werden, dass im Rahmen des Risikomanagements erkannte operative Risiken im Rahmen des IKS verwaltet werden. Die Unterlagen aus dem Risikomanagement sowie dem Internen Kontrollsystem sollten durchgängig sein.

2.2 Ablaufmodelle im Führungssystem ASTRA

Das FS ASTRA beinhaltet die Ablaufmodelle der Prozesse im ASTRA. Dabei wird auf der ersten Ebene unterschieden zwischen Führungsprozessen, Kernprozessen und Supportprozessen. Unter den Kernprozessen findet sich der Prozess „Strasseninfrastruktur“[1]. Dieser wird auf der zweiten Ebene im Wesentlichen unterteilt in die Bereiche „Fertigstellung des beschlossenen NS[2]-Netzes (FSNS)“ sowie „Bau, Ausbau und Betrieb der NS“. In diesen beiden Bereichen finden sich zahlreiche Subprozesse. Im Zusammenhang mit der durchgeführten Prüfung war insbesondere der Subprozess „Investitionscontrolling Bau/UG/Unterhalt“ von Interesse, der im Bereich „Bau, Ausbau und Betrieb der NS“ angegliedert ist. Die übrigen Subprozesse wurden nicht weiter betrachtet. (Vergleiche Prozessmodell im Anhang 3.)

Zielsetzungen des Subprozesses „Investitionscontrolling Bau/UG/Unterhalt“ sind gemäss Ausführungen auf der dritten Ebene im FS ASTRA das Sicherstellen der nötigen Finanzen, die Überwachung der Kredite und die Abrechnung der ausgeführten Bauarbeiten für den Bau und Unterhalt der Nationalstrassen. Um diese Zielsetzung zu erreichen, teilt sich der Subprozess in vier weitere Bereiche. Diese Bereiche enthalten wiederum verschiedene Detailprozesse, die auf der vierten Ebene in Form von Ablaufdiagrammen dargestellt werden. Die relevanten drei der insgesamt vier Bereiche werden nachfolgend kurz umschrieben.

- Kontenplan und Projektstruktur

Innerhalb des Bereiches „Kontenplan und Projektstruktur“ bestehen die beiden Prozessabläufe „Inventarobjekt“ und „Kontenplan führen“. Zielsetzungen dieser Detailprozesse sind gemäss Angaben im FS ASTRA die Änderung eines bestehenden Objektes oder die Erfassung eines neuen Objektes im MISTRA sowie die Sicherstellung der zweckbestimmten Mittelverwendung dank transparenter Aufschlüsselung der Kosten. Im Rahmen dieses Prozesses werden die Grundlagen für die nachgelagerte Abbildung der Projektstrukturen im TDcost erfasst. Im Fokus der Prüfungsarbeiten war die *Schnittstelle zwischen dem MISTRA Basissystem und TDcost* (siehe auch Kapitel 3.1, Kontenplan und Projektstruktur).

- Operatives Investitionscontrolling

Innerhalb des Bereiches „Operatives Investitionscontrolling“ waren die Prozesse *„Rechnungsablauf mit externem Rechnungseingang“* und *„Rechnungseingang mit internem Rechnungseingang“* im Fokus der Prüfungsarbeiten. Zielsetzungen dieser beiden Abläufe sind gemäss Angaben im FS ASTRA Rechnungen zu erfassen, zu genehmigen und zur Zahlung weiterzuleiten (siehe auch Kapitel 3.4, Operatives Investitionscontrolling).

- Investitionsplanung und Kredite NS

Innerhalb des Bereiches „Investitionsplanung und Kredite NS“ waren die Abläufe *„KV[3] in TDcost erfassen“* sowie *„Kredit genehmigen“* im Fokus der Prüfungsarbeiten. Die Ziele der genannten Abläufe sind einen Kostenvoranschlag zu erfassen und zu genehmigen resp. die formelle und materielle

[1] Die weiteren Kernprozesse „Strassennetze“ und Strassenverkehr“ sind im Rahmen der durchgeführten Prüfung nicht von Relevanz und wurden deshalb auch nicht weiter behandelt.

[2] NS = Nationalstrasse

[3] KV = Kostenvoranschlag, entspricht dem genehmigten Kostenrahmen für das Gesamtprojekt

Genehmigung eines Kredites bzw. einer Kreditanpassung sicherzustellen (siehe auch Kapitel 3.2, Investitionsplanung und Kredite NS).

Auf der dritten und vierten Ebene im FS ASTRA *werden* im Zusammenhang mit einer Tätigkeit stehende Risiken mit einer unmittelbar ersichtlichen Ampel angezeigt. Grundsätzlich erfolgt die Anzeige der Risiken auf der vierten Ebene, d.h. bei einer konkreten Tätigkeit innerhalb des dort dargestellten Ablaufdiagrammes. Sofern keine vierte Ebene besteht, erfolgt die Anzeige der Risiken bereits auf der dritten Ebene. Bei Tätigkeiten, denen ein Risiko zugeordnet ist, wird in einem Textfeld zusätzlich darauf hingewiesen, dass eben ein Risiko besteht und deshalb zwingend die Risiko-Kontrollmatrix (RKM) zu konsultieren sei. Eine Kontrollnummer wird ebenfalls angegeben, so dass die entsprechende Kontrolle in der RKM leicht gefunden werden kann. Auf die RKM kann, ausgehend von der risikobehafteten Tätigkeit im FS ASTRA, direkt zugegriffen werden.

	Schlussfolgerung
●	Die gewählte Abbildung der einzelnen Detailprozesse im FS ASTRA beurteilt die EFK konzeptionell als zweckmässig: Innerhalb einer einzigen Anwendung sind die relevanten Prozesse dargestellt und können von allen Mitarbeitenden des ASTRA jederzeit eingesehen werden. Die Anzeige von identifizierten Risiken direkt bei den Tätigkeiten mittels der erwähnten Ampel und der direkte Zugriff auf die RKM stellen eine gute Lösung zur Verbindung der Ablaufdiagramme mit dem dokumentierten IKS dar.

In der Ausgestaltung der RKM erkennt die EFK aber generellen Handlungsbedarf. Dieser wird in den nachfolgenden Kapiteln aufgezeigt.

2.3 Allgemeiner Zweck und Inhalt einer Risiko-Kontrollmatrix

Der Zweck einer RKM liegt zum einen darin, dass den Verantwortlichen ein Gesamtbild über die bestehenden internen Kontrollen ermöglicht wird. Zum anderen ist die RKM ein zentrales Instrument zur Dokumentation des bestehenden IKS. Die finanzrelevanten Geschäftsprozesse einer Verwaltungseinheit sind deshalb in einem ersten Schritt in der RKM aufzunehmen. In einem zweiten Schritt sind die identifizierten Risiken der Prozesse zu beschreiben und zu bewerten. Anschliessend sind pro aufgeführtes Risiko risikominimierende Kontrollaktivitäten zu definieren. Aus Gründen der Übersicht sollte eine RKM eher einfach gehalten werden und sich deshalb auf die wesentlichen Aspekte, also die Schlüsselrisiken und -kontrollen konzentrieren. Um diesem Grundsatz gerecht zu werden, können für die detaillierte und adressatengerechte Dokumentation der durchzuführenden Schlüsselkontrollen allenfalls weiterführende Dokumente (beispielsweise Checklisten, Tätigkeitsbeschreibungen etc.) erarbeitet werden.

2.4 Risiko-Kontrollmatrizen beim ASTRA

Beim ASTRA bestehen drei verschiedene RKM, die vom Bereich Investitionscontrolling in der Abteilung Strasseninfrastruktur im Kontext der durchgeführten Prüfung als relevant beurteilt wurden. Es handelt sich dabei um die RKM für die Geschäftsprozesse „Einkauf Filialen (IC)“, „IT-

Berechtigungen“ und „Einkauf allgemein“. Die ersten beiden RKM wurden im Bereich Investitionscontrolling erarbeitet, die letztgenannte im Bereich Finanzen und Controlling in der Abteilung Direktionsgeschäfte. Dabei wurde das von der EFV im IKS-Leitfaden vom Dezember 2009[4] zur Verfügung gestellte Formular verwendet, das grundsätzlich als zweckdienliches Instrument beurteilt wird.

2.4.1 Risiko-Kontrollmatrix „Einkauf Filiale (IC)“

Die RKM für den Geschäftsprozess „Einkauf Filiale (IC)“ wurde in der Zentrale durch den Bereich Investitionscontrolling als Prozesseigner erstellt. Die RKM an sich ist in den Filialen nicht bekannt. Dies wird aus Sicht der EFK als Schwachstelle beurteilt: Der Kernprozess „Strasseninfrastruktur“ wird zu wesentlichen Teilen in den fünf Filialen des ASTRA abgewickelt und dort werden auch die risikobehafteten Tätigkeiten durchgeführt. Deshalb ist ein Einbezug der Filialen unumgänglich. Letztlich haben die Mitarbeitenden in den Filialen die zur Risikominimierung vorgesehenen Kontrollen in ihrer täglichen Arbeit umzusetzen und deren Durchführung nachweisbar zu dokumentieren. Ansonsten entfalten diese keinerlei Wirkung.

In diesem Zusammenhang zeigt sich eine weitere Schwachstelle der bestehenden RKM: In der RKM besteht die Spalte „durchzuführende Kontrolle um das Risiko zu minimieren“. Darin ist zumindest eine stichwortartige Beschreibung der durchzuführenden Kontrollen zu geben, mittels der das identifizierte Risiko tatsächlich minimiert werden kann. Die in der bestehenden RKM erfassten Angaben sind aber in den meisten Fällen nicht aussagekräftig – im Sinne von klaren Handlungsanweisungen – formuliert. Auf Grund der jetzigen Dokumentation ist bei vielen Risiken deshalb nicht klar, welche Kontrolltätigkeiten effektiv durchzuführen sind. Auch der oftmals vorhandene Verweis auf die IC Weisung ist dabei nicht von weiterem Nutzen für die Mitarbeitenden. Die IC Weisung ist zwar ein sehr umfangreiches und auch hilfreiches Dokument, das vertiefte Informationen zu den ganzen Prozessabläufen des Investitionscontrollings liefert, es sind darin aber weder Risiken noch zugehörige Kontrollen definiert (siehe auch Kapitel 3, Ergebnis der Funktionsprüfungen in ausgewählten Subprozessen). Folglich kann der einzelne Mitarbeitende darin auch keine Informationen bezüglich konkret durchzuführender Kontrolltätigkeiten finden. Wie schon dargelegt, müssen diese Vorgaben den Mitarbeitenden aber gegeben werden. Ansonsten ist der Verweis im FS ASTRA auf die RKM nutzlos. Ergänzend ist in der RKM festzuhalten, wie der Nachweis erbracht werden soll, dass die vorgegebenen Kontrollen auch tatsächlich durchgeführt worden sind. Auch für diese Information ist in der RKM eine separate Zelle vorgesehen, die entsprechend zu überarbeiten ist.

Eine weitere Problematik im Zusammenhang mit der erstellten RKM liegt darin, dass diese nicht mit den Ablaufmodellen im FS ASTRA in Verbindung gebracht werden kann, weil in den beiden Dokumenten unterschiedliche Prozessbezeichnungen verwendet werden. Ganz grundsätzlich ist dabei festzuhalten, dass die Bezeichnungen „Einkauf Filiale (IC)“ sowie die in der RKM aufgeführten Bezeichnungen der Subprozesse im FS ASTRA vergeblich gesucht werden. Bedingt durch die Kontrollnummern im FS ASTRA kann von dort aus zwar die durchzuführende Kontrolle in der RKM

[4] Leitfaden Internes Kontrollsystem – Leitfaden für die Umsetzung der rechtlichen Vorgaben zum Internen Kontrollsystem für die finanzrelevanten Geschäftsprozesse in der Bundesverwaltung

gefunden werden, ausgehend von der RKM können aber die zugehörigen Ablaufmodelle resp. die risikobehafteten Tätigkeiten nur sehr aufwändig oder gar nicht identifiziert werden.

	Schlussfolgerung
■	Die im ASTRA vorliegende RKM „Einkauf Filiale (IC)“ erfüllt die formellen Anforderungen an die Dokumentation des IKS nicht vollumfänglich. Eine Abstimmung mit den Ablaufdiagrammen im FS ASTRA ist ausgehend von der RKM nicht möglich, da die in der RKM aufgeführten Prozesse nicht gleich benannt sind wie diejenigen im FS ASTRA. Die durchzuführenden Kontrollen sind nicht aussagekräftig formuliert, genauso wenig wie die Angaben bezüglich der zu erstellenden Kontrollnachweise. Zudem wird das dokumentierte IKS nicht gelebt, weil es in den Filialen gar nicht bekannt ist. Die Verbindung zwischen der RKM und den in der täglichen Arbeit durchzuführenden Kontrollen konnte folglich nicht hergestellt werden.

Empfehlung 1 (Priorität 1):

Die EFK empfiehlt, die RKM „Einkauf Filiale (IC)“ umfassend zu überarbeiten. Die RKM ist dabei an die Prozessbezeichnungen im FS ASTRA anzupassen (oder umgekehrt), pro identifiziertes Risiko sind Kontrolltätigkeiten im Sinne von eindeutigen Handlungsanweisungen vorzugeben und es ist festzulegen, welche Kontrollnachweise zu erstellen sind. Schliesslich ist die RKM an die Filialen zu kommunizieren, damit die definierten Kontrollen auch tatsächlich durchgeführt werden. Die EFK hält zudem fest, dass diese Empfehlung auch für andere, in diesem Rahmen nicht geprüfte RKM, durchaus Gültigkeit hat und entsprechend umgesetzt werden sollte.

Stellungnahme des ASTRA zur Empfehlung 1:

Die RKM ”Einkauf Filiale (IC)” wird überarbeitet und insbesondere mit den Bezeichnungen im FS ASTRA in Übereinstimmung gebracht. In die IC Weisung wird ein Verweis auf die RKM eingefügt, um die Kohärenz des Risikocontrollings zu dokumentieren.

Da die RKM v.a. eine übersichtliche Zusammenfassung des Geschäfts der Abteilung bietet, sieht das ASTRA eine Schulung der Filialen über die RKM nicht vor. Geschult werden hingegen die daraus abgeleiteten konkreten Massnahmen, die in die verschiedenen Prozessen, Weisungen und Handbüchern einfliessen.

Angaben zu während der Prüfung erkannten Schlüsselkontrollen finden sich im Kapitel 3, Ergebnis der Funktionsprüfungen in ausgewählten Subprozessen.

2.4.2 Risiko-Kontrollmatrix „Einkauf allgemein“

In der RKM „Einkauf Filialen (IC)“ wird für die Detailprozesse „Rechnungszahlung“ und „Stammdaten Kreditoren“ auf die RKM für den Prozess „Einkauf allgemein“ verwiesen. Diese wurde durch den Bereich Finanzen und Controlling erarbeitet und befasst sich hauptsächlich mit den Risiken und Kontrollen unter dem Führungsprozess „Finanzen und Controlling“. Sie wurde deshalb im Rahmen der durchgeführten Prüfung nicht im Detail beurteilt. Informationen zu den relevanten Ri-

siken und Kontrollen, die in der RKM „Einkauf allgemein“ abgebildet werden und dennoch im Rahmen der durchgeführten Prüfung beurteilt wurden, finden sich im Kapitel 3, Ergebnis der Funktionsprüfungen in ausgewählten Subprozessen.

2.4.3 Risiko-Kontrollmatrix „IT-Berechtigungen“

Im Bereich des Prozesses „IT-Berechtigungen“ besteht insbesondere das Schlüsselrisiko, dass die Zugriffsrechte zu umfassend vergeben sind: Mitarbeitende verfügen in einem solchen Fall über Rechte, die sie nicht benötigen oder sogar über Rechte, die sie auf Grund von unvereinbaren Funktionskumulationen gar nicht haben dürften. Ein Beispiel dazu ist in Kapitel 3.4.2, Rechnungsprüfung und -genehmigung aufgeführt.
Das genannte Risiko ist angemessen zu überwachen. Dazu gehört eine entsprechende Kontrolle der Zugriffsrechte bei Ein-/Austritten oder bei Wechseln innerhalb des ASTRA sowie eine periodische Kontrolle über die vergebenen Rechte. Auch hier ist der Grundsatz zu beachten, dass man sich auf die Schlüsselrisiken beschränken sollte. Die bestehende RKM erscheint unter Berücksichtigung dieses Aspektes als zu umfassend.
Weitere Angaben in Bezug auf Schlüsselrisiken und während der Prüfung identifizierte Kontrolllücken im Zusammenhang mit den IT-Berechtigungen sind im Kapitel 4.5, Berechtigungen ersichtlich.

3 Ergebnis der Funktionsprüfungen in ausgewählten Subprozessen

In der Abteilung Infrastruktur besteht die Weisung „Investitionscontrolling Nationalstrassen“ (IC Weisung) als umfangreiches Regelwerk, das die Verantwortlichkeiten und Kompetenzen für die Nationalstrassen-Projekte sowie die diesbezüglichen Prozesse regelt. Die IC Weisung besteht aus drei Teilen. Im Rahmen der durchgeführten Funktionsprüfungen ist insbesondere der Teil C von Bedeutung. Dieser behandelt das Investitionscontrolling auf Projektebene. Die Hauptprozesse im Zusammenhang mit dem Investitionscontrolling Nationalstrassen sind im FS ASTRA abgebildet (siehe auch Kapitel 2.2, Ablaufmodelle im Führungssystem ASTRA). Es liegt aber in der Zuständigkeit der einzelnen Filialen, die Vorgaben der IC Weisung in deren jeweiligen Subprozessen ablauforganisatorisch sicherzustellen. Dies führt dazu, dass alle fünf Filialen eigene Prozessabläufe erarbeitet haben, die sich im Detail voneinander unterscheiden. In der Berichterstattung wird deshalb Bezug genommen auf die Prozessabläufe, wie sie im FS ASTRA allgemein gültig vorgegeben sind (siehe auch Kapitel 3.9, Standardisiertes Prozessvorgehen).

Nachfolgend werden die Feststellungen aus den geprüften Prozessbereichen dargelegt.

3.1 Kontenplan und Projektstruktur

Sämtliche durch das ASTRA betreute Nationalstrassen-Projekte werden im TDcost geführt. Die zentralen Elemente für die Abbildung von Projekten in TDcost sind die Inventarobjekte, die Finanzierungskonten sowie die Kostenarten. Die Finanzierung der verschiedenen Projekte erfolgt durch zwei Finanzierungsquellen (die in separaten Buchungskreisen im SAP abgebildet werden), die fünf verschiedene Finanzierungskonten beinhalten:

Übrige Spezialfinanzierung Strassenverkehr, mit den Finanzierungskonten

- Ausbau / Umgestaltung Nationalstrassen
- Unterhalt Nationalstrassen
- Betrieb Nationalstrassen

Infrastrukturfonds (IF), mit dem Finanzierungskonto

- Engpassbeseitigung Nationalstrassen
- Netzfertigstellung Nationalstrassen[5]

3.1.1 Detailprozess „Inventarobjekt“

In MISTRA gibt es eine GEO-Anwendung mit den Nationalstrassen der ganzen Schweiz. Auf dieser „Strassenkarte“ sind die einzelnen Inventarobjekte (z. B. Abschnitt, Brücke, Tunnel) eingezeichnet und gekennzeichnet. Die Inventarobjekte werden im MISTRA (Mastersystem) durch die Mitarbeitenden der Erhaltungsplanung (EP) der Filialen erstellt und gepflegt. Sie werden periodisch in den Katalog der Inventarobjekte von TDcost importiert. Diese bilden die Basis für die Planung und Durchführung der Bauprojekte und somit auch für die Verträge.

Jedes Inventarobjekt hat eine eigene Nummer, die sich aus den Angaben zum Kanton, zur Strasse, zum Abschnitt und zum Objekt selber zusammensetzt. Die Namenskonvention folgt den Regeln in der IC Weisung.

Im Zusammenhang mit der Erfassung von Inventarobjekten im MISTRA wurden im Rahmen der durchgeführten Prüfungen keine speziellen Prüfungshandlungen vorgenommen. Grundsätzlich ist die EFK aber der Ansicht, dass die richtige Erfassung von Inventarobjekten mittels des 4-Augen-Prinzips sichergestellt werden muss. Wir halten diesbezüglich fest, dass ein Risiko, wonach Inventarobjekte im MISTRA falsch erfasst sein könnten, im FS ASTRA bei der Tätigkeit „Inventarobjekt überprüfen“ nicht angezeigt und auch in der RKM nicht enthalten ist. Eine entsprechende Kontrolle scheint folglich nicht implementiert zu sein.

	Schlussfolgerung
●	Die Pflege der Inventarobjekte erfolgt durch die Erhaltungsplaner in MISTRA. Der Zeitpunkt der Bearbeitung der Infrastrukturobjekte muss keinen direkten Zusammenhang mit einem Projekt haben. Damit jedoch ein Projekt initiiert werden kann, müssen die Infrastrukturobjekte im Katalog von TDcost aktualisiert sein. Die Qualität dieses Kataloges ist wesentlich für die korrekte Abwicklung der Projekte.

[5] Die Netzfertigstellung Nationalstrassen ist im Rahmen der durchgeführten Prüfung nicht weiter relevant, da die Projekte erst nach Abschluss der Bauausführung durch das ASTRA übernommen werden.

3.1.2 Schnittstelle MISTRA und TDcost

Die Schnittstelle wurde im Jahr 2008 erstellt und dient dem Informationsaustausch zwischen TDcost und MISTRA. Dabei werden die Inventarobjekte in TDcost importiert, wobei der Katalog der Inventarobjekte derzeit rund 14.000 Objekte enthält.

Der Prozess für den Datentransfer wird im FS ASTRA unter „Inventarobjekt im TDcost importieren“ beschrieben. Der technische Ablauf ist wie folgt: Auf einem Schnittstellenserver gibt es einen Transfer-Ordner, in dem alle neuen oder aktualisierten Inventarobjekte aus MISTRA in Form von XML-Dateien abgespeichert werden. Es gibt zwei Verzeichnisse auf dem Server: eines für die Filialen und eines für die Zentrale. Die Übertragung der aktualisieren Inventarobjekte ins TDcost wird auf Anfrage der Filialen ausgelöst. Mit einem, durch die Leiterin IC, manuell gestarteten Script werden die Daten vom Schnittstellenserver in die Anwendung TDcost übernommen. In diesen XML-Dateien gibt es einen Schlüssel, der die Identifikation des übertragenen Inventarobjektes ermöglicht. Mitarbeiter, die Zugriff auf das Verzeichnis haben, können die Daten mit einem Text-Editor bearbeiten. Die Datenübertragungen werden in einem Log überwacht. Darin können allenfalls fehlerhafte Datenübermittlungen festgestellt und neu gestartet werden. Die Analyse der Logdateien ist nicht sehr einfach.

Die Schnittstelle wurde vom ASTRA-Team, zusammen mit der Firma Trivadis für den TDcost-Teil umgesetzt. Dabei wurde eine technische Spezifikation für die Schnittstelle erstellt. Es gibt ein Abnahmeprotokoll, das die durchgeführten Tests und Validierungen vor der Produktionsaufnahme beschreibt. Bei jeder Änderung der Anwendung MISTRA werden Tests durchgeführt, um sicherzustellen, dass die Schnittstelle noch funktioniert. Im MISTRA gibt es Anleitungen, die die Verwendung der Anwendung beschreiben. Für die Schnittstelle zu TDcost gibt es keine Dokumentationen.

Zwischenzeitlich wurden nun weitere Arbeiten vorgenommen, um diese Schnittstelle zu automatisieren. Damit soll die manuelle Handhabung zwischen den beiden Systemen vermieden werden und das Risiko einer unvollständigen Datenübertragung minimiert werden.

	Schlussfolgerung
●	Die Schnittstelle verwendet einen Transfer-Server. Damit können die Prozesse der Anwendungen zeitlich entflochten werden. Der Import in TDcost erfolgt durch ein manuelles Starten von einem Script. Die geplante Automatisierung der Schnittstelle kann die Qualität und Aktualität des Kataloges der Inventarobjekte in TDcost verbessern. Die Sicherheit der Schnittstelle wird durch die Berechtigungen auf den Transfer-Server beeinflusst. Die Schnittstelle funktioniert technisch gut und wird mittels Logdateien überwacht.

3.1.3 Detailprozess „Kontenplan führen“

Pro Inventarobjekt wird im TDcost durch die Anwendung des Kontenplans festgelegt, über welches Finanzierungskonto und somit auch über welche Finanzierungsquelle ein geplantes Projekt finanziert wird. Der Anhang 1 zur IC Weisung „Kontenplan Nationalstrassen“ beinhaltet die kontierungsrelevanten Unterlagen. Der umfassende und gut dokumentierte Kontenplan wird nach den Berei-

chen Planung, Unterstützung und Beratung, Projektierung und Bauleitung, Landerwerb, Realisierung, Projektreserve, allgemeine Kosten sowie Erlöse / Einnahmen gegliedert. Die Konten innerhalb dieser Bereiche werden im Rahmen einer Matrix den Hauptkostenarten Projektierung, Landerwerb und Realisierung zugewiesen. Über die Kontierung wird auch automatisch gesteuert, ob die angefallenen Kosten in SAP schliesslich über die Investitionsrechnung oder über die Erfolgsrechnung erfasst werden. Deshalb ist bei jeder Kostenart im Kontenplan zusätzlich angegeben, ob diese aktiviert wird oder nicht.

Der Kontenplan ist mit visuellen Bauplänen (Trasse, Brückenquerschnitt, Brückenlängsschnitt und Tunnelquerschnitt) ergänzt. Die einzelnen Elemente und die dazugehörenden Kostenarten werden darin gut ersichtlich aufgezeigt. Die EFK ist der Meinung, dass mit den vorliegenden Hilfsmitteln den zuständigen Stellen ein wichtiges und detailliertes Arbeitsinstrument bei der Projektplanung zur Verfügung steht.

Änderungen im Kontenplan werden durch das IC der Zentrale erarbeitet und anschliessend vom AC Infrastruktur genehmigt. Nach erfolgter Genehmigung werden die Änderungen durch das IC der Zentrale im TDcost erfasst.

In der RKM sind keine Risiken und keine Kontrollen für die Sicherstellung der richtigen und vollständigen Zuweisung der Kostenarten auf die SAP-Konten vorgesehen.

	Schlussfolgerung
■	Die Richtigkeit von Mutationen im Kontenplan in TDcost, nach erfolgter Genehmigung, sowie die vollständige und richtige Zuweisung der Kostenarten auf die Konten im SAP sind im Rahmen des Investitionscontrolling von zentraler Bedeutung. Es sind im FS ASTRA bei diesem Prozess aber keine Risiken angezeigt oder in der RKM aufgeführt. Das Risiko sollte deshalb im FS ASTRA bei der Tätigkeit „Änderungen KP im ICNS-Tool erfassen“ mittels eines Ampel angezeigt und in der RKM dokumentiert werden. Die vorgängig erforderliche Genehmigung von Mutationen ist nachvollziehbar zu dokumentieren. Das 4-Augen-Prinzip ist dabei sicherzustellen. Ergänzend sollte auch die richtige und vollständige Zuweisung der Kostenarten in TDcost auf die Konten in SAP kontrolliert werden (siehe auch Empfehlung 2).

3.2 Investitionsplanung und Kredite NS

3.2.1 Detailprozess „KV in TDcost erfassen“

Ab der Projektphase „Projektidee“ werden sämtliche Projekte im TDcost abgebildet. Ein in TDcost erfasstes Projekt entwickelt sich hinsichtlich der Projektstruktur in TDcost über alle Projektphasen weiter: Während der Projektphase „Projektidee“ bestehen normalerweise nur ein Inventarobjekt und wenige Kostenarten. In der Phase „Generelles Projekt“ bestehen weiterhin ein Inventarobjekt und wenige Kostenarten. Ab den Projektphasen „Ausführungsprojekt“ und „Detailprojekt“ erhöht sich normalerweise die Anzahl der Inventarobjekte und der Kostenarten. Der Detaillierungsgrad des ursprünglich in TDcost erfassten Kostenvoranschlags entwickelt sich parallel mit dem zuneh-

menden Detaillierungsgrad der Inventarobjekte und der Kostenarten weiter. Um diese Verfeinerung des Kostenvoranschlags vorzunehmen, sind KV-Mutationen notwendig. Die Genehmigungsstufe eines Kostenvoranschlags ist von der Projektphase, der Projektart und dem finanziellen Umfang abhängig. Sämtliche Angaben werden entsprechend der Rollenzuordnung auf Papierunterlagen geprüft und genehmigt sowie anschliessend mittels KV-Mutationen in den IC Filialen im TDcost eingegeben. Die Freigabe von KV-Mutationen erfolgt durch den Bereich IC Zentrale. Eine entsprechende Funktionentrennung ist im System implementiert. Problematisch ist aber, dass verschiedene Mitarbeitende in den Filialen über unvereinbare Funktionskumulationen verfügen. So können zahlreiche Mitarbeitende in den Filialen KV sowohl erfassen und prüfen wie auch genehmigen (siehe auch Kapitel 4.5.1, Die Berechtigungen von TDcost).
Die EFK hat in diesem Zusammenhang primär KV-Mutationen in der Projektphase „Detailprojekt / Massnahmenprojekt“ anhand einzelner Beispiele in den besuchten Filialen geprüft. Sie stellte fest, dass die Basisunterlagen für KV-Mutationen pro Filiale unterschiedlich sind, jedoch insgesamt die notwendigen Informationen, die im System zu erfassen sind, in einer geeigneten Systematik berücksichtigt. Ohne diese formellen Anforderungen werden keine Mutationen im Bereich IC vorgenommen. Im Weiteren wurde festgestellt, dass die verantwortlichen Bereiche bzw. die Mitarbeitenden entsprechend der Unterschriften- und Kompetenzliste die dazugehörenden physischen Unterlagen unterzeichnet haben.

Die richtige Abbildung der genehmigten Kostenvoranschläge im TDcost ist von zentraler Bedeutung. Sie dient unter anderem als Grundlage bei der späteren Erfassung der Rechnungen und somit auch für die Verbuchung in SAP. Im Prozessablauf im FS ASTRA ist kein Risiko angezeigt, nach dem die richtige Eingabe der KV-Mutationen im TDcost in Frage gestellt wird. In der RKM ist auch keine diesbezügliche Kontrolle vorhanden. Die EFK erkennt in diesem Bereich ein klares Risiko für Fehleingaben.

In einzelnen Filialen wurde die EFK darauf hingewiesen, dass gemäss Rollen und Kompetenzen in TDcost die systemtechnische Freigabe der Mutationen durch das IC in der Zentrale erfolgt und somit das 4-Augen-Prinzip eingehalten sei. Das IC Zentrale bestätigt, dass sämtliche Mutationen auf ihre formelle Richtigkeit geprüft werden und somit die richtige Erfassung im System sichergestellt ist.

	Schlussfolgerung
■	Die richtige Abbildung der genehmigten KV-Mutationen im TDcost ist von zentraler Bedeutung. Das Risiko, dass Mutationen falsch erfasst werden könnten, ist weder im FS ASTRA angezeigt noch in die RKM aufgenommen. Das Risiko von falschen Mutationen sollte deshalb im FS ASTRA bei den Tätigkeiten „KV erfassen“ sowie „KV-Mutationen erfassen“ angezeigt und in der RKM dokumentiert werden.

Empfehlung 2 (Proirität 2):

Die EFK empfiehlt, die richtige Erfassung von allen Mutationen im TDcost mittels 4-Augen-Prinzip sicherzustellen. Dabei ist darauf zu achten, dass Kontrollen nachgelagert und nicht zeitgleich zur

Erfassung erfolgen. Die Verantwortung für diese Kontrolle sollte dabei eindeutig geregelt werden und die Kontrolle ist nachweisbar zu dokumentieren.

Stellungnahme des ASTRA zur Empfehlung 2:
Die Berechtigungen in TDcost werden so angepasst, dass das 4-Augen-Prinzip bei der Erfassung und der Kontrolle der KV-Mutationen gewährleistet ist.

3.3 Detailprozess „Kredit genehmigen“

3.3.1 Manuelle Kontrollen

Mit den Krediten werden die genehmigten Mittel im TDcost tatsächlich freigegeben. Die Kredite werden pro Hauptkostenart (Projektierung, Landerwerb, Realisierung) und pro Finanzierungskonto geführt. Wenn ein KV in TDcost erfasst worden ist, muss auch immer ein Kredit zugewiesen werden. Kredite werden entsprechend den Kenntnissen des Projektes in TDcost freigegeben. Nebst den Krediten für das Projekt gibt es auch die jährlichen Voranschlagskredite. Sie legen fest, wie viel in einem Jahr für ein Projekt ausgegeben werden darf. Die Zuteilung der zur Verfügung stehenden Mittel auf die einzelnen Projekte erfolgt gemäss den langfristigen Bau- und Erhaltungsprogrammen. Auch in diesem Bereich bestehen im TDcost unvereinbare Funktionskumulationen (siehe auch Kapitel 4.5.1, Die Berechtigungen von TDcost).

Für die laufende Steuerung und Führung der Kredite bzw. der Projekte bestehen übergreifende, standardisierte Investitionsreportings, die in vorgegebenen Intervallen zu erstellen sind und der Abteilung Zentrale zugestellt werden müssen[6]. Zusätzlich werden in den Führungsrapporten der Abteilung Infrastruktur die Projektsituationen systematisch besprochen. Dies stellt eine transparente und laufende Kreditkontrolle sicher.

Ergänzend führen die Filialen unterschiedliche Reportings, die sie für die Steuerung und Führung der Projekte innerhalb ihrer Filiale benötigen. Die Berichte basieren auf den Daten von TDcost und werden einerseits in einer Excel Datei erstellt oder andererseits mittels Datawarehouse erzeugt. In der Filiale Bellinzona wird beispielsweise die Projektübersicht – Kostenentwicklung – alle zwei Wochen in der Filialsitzung besprochen. Diese laufende Kostenübersicht macht es möglich, dass situativ auf die Bauvorhaben bzw. den sich abzeichnenden Finanzierungsbedarf reagiert werden kann. Sofern notwendig können Kreditmutationen rechtzeitig vorgenommen werden. Im Weiteren führt die Filiale für grössere Projekte eine Excel Datei mit den aufgelaufenen Projektkosten sowie sich abzeichnenden Mehrkosten, die im TDcost noch nicht berücksichtigt sind. Ziel dieser Auswertung ist es, über detaillierte Informationen bezüglich zusätzlicher Projektkosten zu verfügen.

Mit dem standardisierten Investitionsreporting ist ein zentral definierter und systematisch zu erstellender Bericht vorhanden, der die finanzielle Situation der Projekte über sämtliche Filialen wiedergibt. In den Filialen werden ergänzend unterschiedliche und gute Hilfsmittel zur Überwachung der finanziellen Mittel, d.h. der Kredite eingesetzt. Mit dem seit dem Jahr 2012 im Einsatz stehenden Datawarehouse können individuelle Auswertungen erstellt werden. Zur Nutzung des bestehenden

[6] Vergleiche dazu Kapitel 8 in der IC-Weisung

Synergiepotentials könnten die Bedürfnisse der Filialen konsolidiert werden und überprüft werden, ob diese mittels standardisierten Berichten aus dem Datawarehouse erfüllt werden könnten. Auf die Erstellung von manuellen Auswertungen sollte nach Möglichkeit verzichtet werden, da diese fehleranfällig sind (siehe auch Kapitel 3.9, Standardisiertes Prozessvorgehen).

	Schlussfolgerung
●	Die EFK stellt fest, dass die Kreditführung und Kreditsteuerung in den Filialen wie auch in Zusammenarbeit mit der Zentrale zweckmässig erfolgt. Eine laufende Überwachung der Kredite ist sichergestellt.

3.3.2 Automatische Kontrollen

Im TDcost sind verschiedene Kostenschwellen (Warnung) und Kostensperren (Sperre) implementiert. Diese funktionieren aus technischer Sicht zuverlässig.

Wenn eine Kostensperre angezeigt wird, ist ein Kredit aufgebraucht und es können keine Rechnungen mehr bezahlt werden. Die Kostensperre kann in solchen Fällen nur mittels Kreditmutationen oder Mutation von Voranschlagskrediten beseitigt werden. Diese können durch den Bereichsleiter einer Filiale (Kredite) oder in der Zentrale (Voranschlagskredite) freigegeben werden.

Bei der Überschreitung von Kostenschwellen werden lediglich Warnungen angezeigt. Diese haben keine weiteren Folgen. Je nach Ausgestaltung der Kreditführung und der Kreditsteuerung sowie der Prozessausgestaltung im Bereich der Rechnungsgenehmigung in den Filialen sind diese Meldungen nicht von weiterem Nutzen oder werden gar nicht den verantwortlichen Mitarbeitenden (Projekt- und Bereichsleiter) zur Anzeige gebracht. Finanzierungsengpässe sollten, bedingt durch die Kreditführung und Kreditsteuerung, bereits vor einer Kostensperre erkannt und behoben werden. Denn wenn eine Kostensperre angezeigt wird, sind die Kosten bereits angefallen und müssen schliesslich auch beglichen werden.

Die EFK hat die im System TDcost enthaltenen Kontrollen hinsichtlich der hinterlegten Kostenschwellen geprüft. Aufgrund der Testergebnisse kann bestätigt werden, dass zum Zeitpunkt der durchgeführten Tests die programmierten Kontrollen, wie dies in der IC-Weisung beschrieben ist, technisch funktionieren. Insbesondere fokussierte sich die Prüfung auf die definierten Kostensperren, weil diese die Weiterverarbeitung verhindern. Bei Erreichung eines entsprechenden Sperrwerts können beispielsweise keine Verträge mehr erfasst werden. Bei den geprüften Sperrwerten handelt es sich um die aktuell hinterlegten Werte.

	Schlussfolgerung
●	Die Anzeige von Meldungen bei Überschreitung einer Kostenschwelle oder die Erstellung von Kostensperren im TDcost funktionieren technisch zuverlässig. Bei vorliegen einer Kostensperre können ohne vorgängige Kreditmutation keine Rechnungen mehr bezahlt werden. Diese automatische Kontrolle erfolgt aber eigentlich zu spät im Prozess, da zu diesem

	Zeitpunkt die zu bezahlende Leistung bereits erbracht worden ist und schliesslich auch bezahlt werden muss. Von zentraler Bedeutung sind aber die vorgelagerten manuellen Kontrollen.

3.4 Operatives Investitionscontrolling

3.4.1 Detailprozesse „Rechnungsablauf mit externem und internem Rechnungseingang“

Der Rechnungsablauf ist in den fünf Filialen unterschiedlich geregelt. Es gibt Filialen, die über einen zentralen Rechnungseingang verfügen. Dadurch wird sichergestellt, dass jede Rechnung zuerst beim ASTRA eingeht. Erst nach der (Vor-) Erfassung im TDcost werden die Originalrechnungen zur Rechnungsprüfung an die BHU weitergeleitet. Mittels einer manuell geführten Excel-Liste können die Rücklauffristen der zur Überprüfung an externe Stellen verschickten Rechnung überwacht werden. Dieses Vorgehen minimiert das Risiko von nicht erfassten oder doppelt erfassten Rechnung.

Zwar ist im TDcost eine automatische Kontrolle implementiert, die doppelt erfasste Rechnungen aufdecken kann: Wenn unter dem gleichen Vertrag die gleiche Rechnungsnummer erfasst wird, kann das System dies erkennen. Doch schon bei nur geringfügigen Abweichungen in der erfassten Rechnungsnummer, z.B. einem Leerschlag oder einer Abkürzung der Rechnungsnummer (weil nicht genügend Zeichen im auszufüllenden Feld zur Verfügung stehen), fällt diese Kontrolle aus. Sie kann deshalb nicht als ausreichend wirksam beurteilt werden, um die Doppelerfassung von Rechnungen präventiv zu vermeiden.

Bezüglich der nicht erfassten Rechnungen bestehen ohne zentralen Rechnungseingang keine Kontrollen, weshalb die Risiken von doppelt erfassten oder nicht erfassten Rechnungen nicht ausreichend abgedeckt werden. Durch die Implementierung eines zentralen Rechnungseingangs können diese Risiken deutlich herabgesetzt werden. Zudem können die Arbeiten im Zeitpunkt des Jahresabschluss vereinfacht werden, da bereits eingetroffenen Rechnungen zuverlässig ermittelt werden. Die zu bildende Abgrenzung kann dadurch nur noch auf erbrachte aber noch nicht in Rechnung gestellte Arbeiten fokussiert werden, was die Zuverlässigkeit der Abgrenzung erhöhen wird (siehe auch Kapitel 3.7, Jahresabschluss). Ein zentraler Rechnungseingang ermöglicht auch, dass nach dem Rechnungseingang zuerst eine formelle Prüfung der Rechnung in den Filialen vorgenommen werden kann. Der Kontrollnachweis für die formelle Prüfung kann mittels Visum auf der Rechnung resp. dem Rechnungsdeckblatt sehr einfach erbracht werden.

Obwohl im FS ASTRA sowohl der Rechnungsablauf mit zentralem Rechnungseingang als auch mit dezentralem Eingang beschrieben sind, ist der Prozess mit zentralem Rechnungseingang aus den aufgeführten Gründen aus Sicht der EFK zu bevorzugen. Sehr umfassende Unterlagen zur Ausgestaltung eines zentralen Rechnungseingangs bestehen in der Filiale Winterthur, die für die anderen Filialen bei einer allfälligen Umstellung von grossem Nutzen sein könnten. Im Hinblick auf eine verstärkte Abwicklung der Prozesse und Kontrollen im System ist eine einheitliche Umsetzung bei den Filialen unbedingt anzustreben.

	Schlussfolgerung
■	Das Risiko von nicht erfassten oder doppelt erfassten Rechnungen ist in den Filialen ohne zentralen Rechnungseingang nicht ausreichend abgedeckt. Die im System implementierte Kontrolle ist nicht wirksam. Das Vorgehen sollte standardisiert und der Rechnungseingang zentralisiert werden *(siehe auch Kapitel 3.9 Standardisiertes Prozessvorgehen).*

Empfehlung 3 (Priorität 2):

Die EFK empfiehlt, den Rechnungseingangsprozess hinsichtlich Abgrenzungen sowie nicht oder doppelt erfassten Rechnungen zu überprüfen. Eine verbindliche Vorgabe des Rechnungsablaufs mit einheitlichem Rechnungseingang bei allen ASTRA Filialen würde zu einer besseren Kontrolle führen. Zur Optimierung des Prozesses sollte zudem geprüft werden, ob die manuelle Fristenkontrolle der zur Prüfung extern verschickten Rechnungen nicht durch eine automatisierte Lösung ersetzt werden könnte, die – gemäss ungeprüfter Aussage – im TDcost bereits vorhanden sein sollte.

Stellungnahme des ASTRA zur Empfehlung 3:

Der Rechnungsablauf wird dahingehend vereinheitlicht, dass der externe Rechnungseingang generell verbindlich erklärt wird. Damit erübrigt sich auch die manuelle Fristenkontrolle für extern verschickte Rechnungen.

3.4.2 Rechnungsprüfung und -genehmigung

In den meisten Fällen müssen die Rechnungen zuerst durch externe Stellen materiell geprüft werden. Bei den Prüfern handelt es sich um die Bauherrenunterstützung und/oder um die örtliche Bauleitung. Mittels manueller Unterzeichnung der Rechnung resp. des Rechnungsdeckblattes wird die materielle Richtigkeit bestätigt. Anschliessend wird die Rechnung an die ASTRA Filiale zur nachgelagerten Genehmigung durch den Projektleiter und den Bereichsleiter zurückgeschickt. Diese bestätigen mit ihrer Unterschrift auf der Rechnung nochmals die materielle Richtigkeit der Rechnung.

Die Rechnungsprüfung und –genehmigung aller Parteien wird mittels Unterschrift auf dem Originaldokument und dem Rechnungsdeckblatt nachweisbar durchgeführt. Das im Rahmen der Rechnungsprüfung geforderte Vier-Augen-Prinzip ist somit grundsätzlich sichergestellt. Die diesbezügliche Stichprobe in der Filiale Winterthur hat gezeigt, dass diese manuelle Kontrolle dort grundsätzlich als wirksam beurteilt werden kann. Eine Schwachstelle liegt aber darin, dass die vorhandenen Visa oder Unterschriften (insbesondere der externen Prüfer) durch Dritte (Revision) nicht auf ihre Gültigkeit hin überprüft werden können. Es bestehen keine entsprechenden Unterschriftenlisten, das 4-Augenprinzip kann nur durch die Projektleiter und Bereichsleiter wahrgenommen werden, da diese meist die Unterzeichnenden kennen. Die Kontrollen basieren somit auf Vertrauensbasis. Zudem kann diese eigentlich wirksame Kontrolle durch die Abbildung des manuellen Genehmigungsprozesses beim Übergang ins TDcost sehr einfach umgangen werden:

Im TDcost muss anlässlich der Bearbeitung der eingegangen Rechnungen in verschiedenen Feldern (namentlich in den Feldern „geprüft am“ und „genehmigt am“) ein Datum eingetragen werden.

Wenn das Feld „genehmigt am“ von der Filiale ausgefüllt ist, erkennen die dafür zuständigen Mitarbeitenden in der Zentrale diese Rechnung als bereit für die Freigabe. Die Berechtigungen in den Filialen sind so vergeben, dass zahlreiche Mitarbeitende in den Filialen im TDcost Rechnungen sowohl erfassen und prüfen, als auch genehmigen können. Es besteht in diesem Bereich keine wirksame Funktionentrennung durch angepasste IT-Berechtigungen (siehe auch Kapitel 4.5.1, Die Berechtigungen von TDcost). Es gilt anzumerken, dass die Felder „geprüft am“ und „genehmigt am“ nicht in allen Filialen von den gleichen Personen ausgefüllt werden. Beispielsweise in Winterthur werden alle Daten von einer Mitarbeiterin im TDcost erfasst. Die Erfassung im System erfolgt dort, wenn die Papierrechnung den manuellen Genehmigungsprozess vollständig durchlaufen hat. In anderen Filialen werden die Daten „geprüft am“ und „genehmigt am“ auch durch Projektleiter und Bereichsleiter ausgefüllt. Wer die Daten im System erfasst, ist – bedingt durch die fehlende Funktionentrennung – eigentlich unerheblich. Dies gilt insbesondere auch deshalb, weil keine Auswertung darüber möglich ist, wer die entsprechende Mutation im System vorgenommen hat (siehe auch Kapitel 4.3.2 Eine Historisierung der Transaktionen wurde bisher in TDcost nicht eingesetzt).

Eine wirksame Funktionentrennung besteht lediglich zur Zentrale. Mitarbeitende in den Filialen können Rechnung erfassen, prüfen und genehmigen, aber nicht zur Zahlung freigeben. Die entsprechende Berechtigung haben nur Mitarbeitende in der Zentrale. Aber auch diese Trennung stellt kein ausreichendes 4-Augen-Prinzip sicher, da in der Zentrale keine materiellen Rechnungsprüfung durchgeführt werden kann (siehe auch Kapitel 3.4.5 Rechnungsfreigabe).

	Schlussfolgerung
▲	Der ordentliche Genehmigungsprozess auf den Originalrechnungen wird im System durchbrochen. Es ist nicht ausreichend sichergestellt, dass im System zur Zahlung freigegebene Rechnungen auch tatsächlich von den dafür zuständigen Mitarbeitenden (namentlich Projekt- und Bereichsleiter) geprüft und genehmigt worden sind. Die Filialen tragen die Verantwortung dafür. Es bestehen unvereinbare Funktionskumulationen in den Rollen der Filialen.

Empfehlung 4 (Priorität 2):

Die EFK empfiehlt, die Berechtigungen für die Felder „geprüft am“ und „genehmigt am“ weiter einzuschränken. Optimal wäre eine Lösung im TDcost, bei der beispielsweise die Projektleiter Rechnungen nur prüfen und Bereichsleiter Rechnungen nur genehmigen können. Wesentlich ist, dass das 4-Augenprinzip durch zwei unabhängige Personen einhalten wird. Die Rechte im F-ICR sollten auf die Erfassung von Rechnungen eingeschränkt werden.

Stellungnahme des ASTRA zur Empfehlung 4:

Die Berechtigungen in TDcost werden so angepasst, dass das 4-Augen-Prinzip bei der Prüfung und der Genehmigung der Rechnungen gewährleistet ist und dass F-IC lediglich für die Erfassung der Rechnungen zuständig ist.

3.4.3 Wichtige ESR-Zahlungsdaten können ungeprüft überschrieben werden

Eine der zentralen Funktionen im TDcost beinhaltet die Erfassung sowie die Freigabe von Rechnungen. Nach der Freigabe erfolgt die Zahlung weitgehend automatisch, sofern alle Daten korrekt sind und der Kreditor im System gültig sowie der Zahlweg richtig ist.

Bei Rechnungen können die Zahlwege entweder über die im Kreditorenstamm hinterlegten Bankverbindungen oder über eine ESR-Zeile, d. h. über die standardisierte Form von Einzahlungsscheinen mit Referenznummern (ESR), erfasst werden. Zur Erfassung der ESR-Zeile können die Einzahlungsscheine entweder mit einem Belegleser eingelesen oder manuell erfasst werden. Nach dem Einlesen können die ESR-Daten, die sich aus einer standardisierten Form von Bank-Konto-Nummer, Betrag, Bankverbindung sowie Belegnummer ergeben (die in sich selber validiert werden), überschrieben werden. Während dem der Zahlweg über die hinterlegte Bankverbindung nicht abgeändert werden kann, wird die ESR-Zeile ohne weitere Prüfung übernommen. Falls nun die Syntax der ESR-Zeile (also die Prüfung in sich selber) eine gültige Bankverbindung darstellt, wird die Zahlung nach der Übergabe automatisch auf dieses Bankkonto vorgenommen. Ob die Bank die Übereinstimmung des Kreditors mit dem Zahlungsbegünstigten validiert, kann in einzelnen Fällen vermutet werden, ist jedoch nicht sichergestellt. Dadurch besteht ein erhebliches Risiko, dass Zahlungen (insbesondere unter Anwendung von krimineller Energie) an nicht berechtigte Firmen oder Personen ausgeführt werden könnten.

	Schlussfolgerung
▲	Die EFK beurteilt die Möglichkeit der Überschreibung der ESR-Zeile als ein erhebliches Risiko für fehlgeleitete Zahlungen. Eine Risikominimierung ist praktisch nur gegeben, wenn bei der Zahlungsauslösung eine zusätzliche Validierung oder Überprüfung des ESR-Zahlwegs vorgenommen wird. Optimaler erachtet die EFK, wenn konsequent die fix hinterlegte Bankverbindung, die in TDcost nicht verändert werden kann, genutzt werden muss.

Empfehlung 5 (Priorität 1):

Die EFK empfiehlt, bei der Verwendung der Zahlmöglichkeit mittels Einzahlungsscheinen mit Referenznummern (ESR) zusätzliche Prüfungen der ESR-Erfassungszeilen, z. B. mittels einem 4-Augen-Prinzip, nachprüfbar durchzusetzen oder ansonsten nur konsequent die fix hinterlegten Bankverbindungen des Kreditors zu nutzen. Diese Kontrolle kann am Besten implementiert werden, wenn die Rechnungserfassung und die Prüfung resp. die Genehmigung durch die Berechtigungen wirksam getrennt werden.

Stellungnahme des ASTRA zur Empfehlung 5:

”Die Prüfung der ESR-Erfassungszeile wird als Kontrolltätigkeit in den FS-Prozess aufgenommen, das 4-Augen Prinzip in der Erfassung und der Kontrolle durchgesetzt.

Der Verzicht auf ESR kann dagegen nicht in Betracht gezogen werden, da es sich dabei um ein gerade bei KMU weit verbreitetes Zahlungssystem handelt.”

3.4.4 Rechnungsscanning und Verlinkung in FABASOFT

Die Originalrechnungen (meist nur das Rechnungsdeckblatt) werden eingescannt und mittels einem Link zu FABASOFT im TDcost hinterlegt. Grundsätzlich bietet FABASOFT eine Versionenkontrolle und ein Log der Mutationen. Das ASTRA hat zudem Namenskonventionen festgelegt.

Dieses Scanning erfolgt in den Filialen nicht zum gleichen Zeitpunkt. Die Filiale Winterthur scannt die Rechnungen ein, wenn diese von allen zuständigen Stellen genehmigt worden sind und zur Freigabe an die Zentrale weitergeleitet werden. Dieses Vorgehen entspricht dem allgemein gültigen Ablaufdiagramm im FS ASTRA. In der Filiale Winterthur wird mittels einer Excelliste und mit einem entsprechenden Vermerk im Feld „Bemerkungen“ nachvollziehbar, wo sich die Rechnung befindet (siehe auch Kapitel 3.4.1 Detailprozesse „Rechnungsablauf mit externem und internem Rechnungseingang). Ein Scanning der Rechnungen anlässlich des Rechnungseingangs ist deshalb nicht notwendig. Bei Bedarf, d.h. wenn eine Rechnung tatsächlich verloren gehen würde, könnte beim Rechnungssteller eine neue Rechnung verlangt werden.

Bei anderen Filialen werden die Rechnungen beim Rechnungseingang, d.h. vor dem Genehmigungslauf gescannt. Dieses Scanning soll sicherstellen, dass die Rechnungen bei Bedarf zumindest elektronisch noch vorhanden sind. Wenn die Genehmigung erfolgt ist, werden einzelne Seiten des elektronischen Dokumentes (PDF-Format mit Acrobat Pro) ausgetauscht. Dieses Vorgehen birgt Risiken, da offensichtlich einzelne Seiten ausgetauscht werden, ohne dass ein Nachvollzug möglich ist. Verbunden mit der fehlenden Funktionentrennung im System resultieren aus diesem Vorgehen verschiedene Risiken. Rechtsrelevant ist immer die Papierrechnung. Die elektronische Ablage ist für die Freigabe der Rechnung erforderlich.

	Schlussfolgerung
■	Nach dem dokumentierten Prozess für die Verwaltung von Rechnungen, sollten Rechnungen einmal gescannt werden, wenn diese auf dem Dokument ordentlich genehmigt worden sind. Die Manipulation von in FABASOFT abgelegten Dokumenten ist risikobehaftet. Ein Dokumentenmanagementsystem hat den Zweck, Dokumente sicher zu speichern und die Veränderungen aufzuzeigen. Die Praxis, mit Acrobat Pro einzelne Seiten auszutauschen, muss unterbunden werden.

Empfehlung 6 (Priorität 2):

Die EFK empfiehlt, entsprechend dem Ablaufdiagramm im FS ASTRA die Rechnungen nur einmal, nach erfolgter Genehmigung einzulesen. Die Unterlagen mehrmals einzulesen bringt weitere Risiken mit sich, die leicht vermieden werden können. Die EFK empfiehlt, die Manipulation von in FABASOFT abgelegten Dokumenten zu unterbinden.

Stellungnahme des ASTRA zur Empfehlung 6:
Die Rechnung wird nach Vereinheitlichung des Rechnungsablaufs nur noch einmal, d.h. nach erfolgter interner und externer Genehmigung, eingelesen (vgl. Empfehlung 3).

3.4.5 Rechnungsfreigabe im IC der Zentrale

Die Mitarbeitenden im IC der Zentrale können die materielle Richtigkeit einer Rechnung nicht vollumfänglich prüfen. Sie können lediglich einige Plausibilitätschecks durchführen. Je grösser die Erfahrung eines Mitarbeitenden, desto wirksamer werden wohl diese nicht standardisierten Checks. Es ist aber festzuhalten, dass die meisten Rechnungen ohne weiterführende Prüfungen durch das IC der Zentrale freigegeben werden. Es ist also zwingend, dass die materielle und formelle Richtigkeit sowie die richtige Verbuchung einer Rechnung durch die Filialen sichergestellt werden muss. Es ist festzuhalten, dass die Filialen häufig auf die nachgelagerte Kontrolle in der Zentrale verweisen. Die Filialen sind deshalb erneut darüber zu informieren, dass es sich nicht um eine vollständige und umfassende Kontrolle handelt: Die Verantwortung dafür, dass nur korrekt erfasste und genehmigte Rechnungen zur Zahlung weitergeleitet werden, liegt eindeutig und vollständig bei den Filialen.

Nach Erfassung des Datums „freigegeben am“ durch die Zentrale werden die Rechnungen ins SAP übernommen und anschliessend im Rahmen des herkömmlichen Prozess „Zahlungsmanagement“ bezahlt. Dieser Prozess wurde nicht weiter geprüft, da er in SAP auf dem Bundesstandard abgewickelt wird (siehe auch 3.5, Detailprozess „Rechnungszahlung“ (Finanzen und Controlling)).

	Schlussfolgerung
■	Die Rechnungsfreigabe in der Zentrale stellt keine umfassende Kontrolle dar. Materielle Prüfungen können in der Filiale auch nicht durchgeführt werden. Es ist deshalb in den vorgelagerten Prozessschritten durch die Filialen sicherzustellen, dass nur geprüfte, genehmigte und korrekt erfasste Rechnungen zur Freigabe an die Zentrale gemeldet werden. Bedingt durch die vorgängig dargelegten Schwachstellen im Prozess ist dies momentan nicht ausreichend nachgewiesen. Die Filialen sind ausdrücklich darauf hinzuweisen, dass in der Zentrale im Rahmen der Rechnungsfreigabe keine materiellen Prüfungen durchgeführt werden können.-Es handelt sich dabei hauptsächlich um einen „Prozessanstoss“ im TDcost, damit die Rechnungen über die Schnittstelle ins SAP übernommen werden können sowie um eine stichprobenweise durchgeführte Plausibilisierung der Rechnungen. Die Filialen müssen in ihren Prozessen die notwendigen formellen und materiellen Kontrollen implementieren und nachweisbar durchführen. Ergänzend sollte überprüft werden, ob dieser Prozessanstoss durch das IC der Zentrale überhaupt zweckmässig ist.

3.4.6 SAP

Die Datenabstimmung zwischen TDcost und SAP wird zwischen IC Zentrale sowie dem Bereich Finanzen und Controlling in enger Zusammenarbeit erstellt. Die monatliche Kontrolle wird dokumentiert, Differenzen zwischen beiden Systemen werden festgehalten. Dieser Prozess ist eine Schlüsselkontrolle, die durch Finanzen und Controlling nachgewiesen wird. Mit dem Jahresabschluss 2011 wurde die technische Überleitung von TDcost auf SAP durch die EFK geprüft, es bestanden formale Mängel, die mit dem Abschluss 2012 bereinigt wurden.

	Schlussfolgerung
●	Die Schnittstelle von TDcost zu SAP funktioniert gut und wird laufend überwacht.

3.4.7 Sicherheitsüberprüfungen der Schnittstellenserver haben eklatante Lücken aufgedeckt

Eine Überprüfung des Systems TDcost und der eingesetzten IT-Komponenten wurde im Herbst 2008 durch eine externe Firma in Zusammenarbeit mit dem Finanzinspektorat (FISP) durchgeführt. Dabei wurden massgebliche Schwachstellen, insbesondere hinsichtlich des Datenübergabe-Servers WINSCP, über welchen alle Datenkommunikationen der Schnittstellen zwischen TDcost und SAP laufen, festgestellt. In der Zwischenzeit wurden nach Aussage des Leistungserbringers BIT einige Verbesserungen durchgesetzt, ohne dass weitere Bestätigungen und Nachweise diesbezüglich vorhanden sind.

Da dies nicht im Prüfungsumfang des vorliegenden Auftrages lag, wurden keine weiteren Prüfungen durchgeführt.

Aus Sicht der Risikominimierung sollte das ASTRA ein wesentliches Interesse haben, entsprechende Sicherheitslücken zu schliessen. Ob die gemäss BIT umgesetzten Verbesserungen tatsächlich vorgenommen wurden, müsste daher aus Sicht der EFK durch eine weitere Untersuchung erhärtet werden. Die EFK behält sich vor, entsprechende Aspekte in zukünftigen Prüfungen aufzunehmen.

	Schlussfolgerung
■	Die Sicherheit der Netzwerke und speziell des Servers WINSCP ist sehr wichtig. Auch wenn die Kontrollen der Schnittstelle zwischen TDcost und SAP keine Hinweise zu weiteren Sicherheitsproblemen ergaben, ist eine Prüfung der Massnahmen des BIT zur Erhöhung der Sicherheit des Servers notwendig.

3.5 Detailprozess „Rechnungszahlung“ (Finanzen und Controlling)

Der Prozess der Rechnungszahlung obliegt dem Bereich Finanzen und Controlling. Da er hauptsächlich im SAP System abläuft und elektronisch genehmigt wird, wurden aus Risikoüberlegungen in diesem Prozess keine weiteren Prüfungshandlungen vorgenommen. Aus Sicht der EFK ist es von zentraler Bedeutung, dass die Rechnungen korrekt genehmigt und verbucht ins SAP übergehen, danach sind materiell keine Kontrollen mehr möglich. Rein im Prozess der Rechnungszahlung sind keine Schlüsselrisiken erkennbar.

3.6 Detailprozess „Stammdaten Kreditoren“ (Finanzen und Controlling sowie Filialen)

Zur Neuerfassung von Kreditoren Stammdaten oder für die Mutation von bestehenden Kreditoren Stammdaten wird eine Excel-Liste geführt. Darin erfassen die Mitarbeitenden der Filialen ihre Anträge. Neuerfassungen oder Mutationen werden farblich unterschiedlich gekennzeichnet. Die Anträge werden im IC Zentrale soweit möglich geprüft (z.B. insbesondere Abstimmung mit dem Zentralen Firmenindex, ansonsten bestehen kaum Prüfmöglichkeiten). Sofern sie als korrekt beurteilt werden, werden sie an den Bereich Finanzen und Controlling zur Erfassung in SAP gemeldet. Eine aktive Rückmeldung bezüglich der Durchführung erfolgt bewusst nicht, vorgenommene Änderungen können in der Excel-Liste eingesehen werden.

	Schlussfolgerung
▲	Es besteht eine Funktionentrennung zwischen den Prozessen Kreditoren erfassen resp. mutieren und der Rechnungserfassung. Diese, wie auch die Prüfungen im IC der Zentrale, stellen aber nicht ausreichend sicher, dass nur berechtigte Anträge zur Erfassung oder Mutation von Kreditoren bearbeitet werden. Dadurch haben einzelne Mitarbeitende in den Filialen zu viele Rechte und können Anträge zur Erfassung von Kreditoren erstellen, Rechnungen erfassen sowie prüfen. Es besteht eine unvereinbare Funktionskumulation, da anlässlich der Rechnungsfreigabe in der Zentrale lediglich eine stichprobenweise Plausibilisierung der Rechnungen und keine Prüfung vorgenommen wird. Diese sollte dringend behoben werden.

Empfehlung 7 (Priorität 1):

Die EFK empfiehlt, die Anträge zur Erfassung oder zur Mutation von Kreditorenstammdaten mit einer Genehmigung in der Filiale zu versehen (4-Augen-Prinzip), damit die Notwendigkeit von Mutationen und Neuerfassungen materiell geprüft werden kann.

Stellungnahme des ASTRA zur Empfehlung 7:

Die Kreditoren-Antragsliste im GEVER ASTRA wird so angepasst, dass das 4-Augen-Prinzip bei der Erfassung bzw. bei Mutationen und der Kontrolle von Kreditorenstammdaten gewährleistet ist.

3.7 Jahresabschluss

Für die Erstellung des Jahresabschlusses ist in Teil C, Anhang 15d, der IC Weisung eine Terminliste vorgegeben. Sie zeigt, welche Arbeiten von den verschiedenen Bereichen vorzunehmen sind. Dieser Terminplan ermöglicht es den Filialen intern die nötigen Massnahmen vorzunehmen. In den geprüften Filialen werden unterschiedliche Vorgehensweisen zur Einhaltung des Terminplans angewendet.

Die zeitlichen Abgrenzungen auf Ende Jahr wurden in der Vorgehensweise und Unterlagenerstellung durch die IC Zentrale definiert und standardisiert. Hierzu liegt die Anleitung zur Abgrenzung von Leistungen Nationalstrassen vor, die den Zweck, die Auswirkungen, den Ablauf und weiterfüh-

rende Erläuterungen beinhaltet. Die Abgrenzungen werden pro Projekt bzw. pro Vertrag ausgewiesen und aggregiert. Die Evaluierung der Daten obliegt im Zuständigkeitsbereich des Projektleiters, das IC plausibilisiert die Daten. Es wurde festgestellt, dass der definierte Ablauf von allen Filialen eingehalten wurde. Kleinere Abweichungen in der Vorgehensweise sind vorhanden, für die Datenerstellung und -berechnung jedoch irrelevant. Eine Nachprüfung der für den Jahresabschluss 2012 gebildeten Abgrenzung ist gemäss Anleitung bis Ende Mai 2013 vorzunehmen. Im Zeitpunkt der Revision wurden diese Plausibilitäten noch nicht überall vorgenommen. Das FISP ASTRA hat ebenfalls Prüfungen zu den zeitlichen Abgrenzungen gemacht.

3.8 Aktivierung von Projektkosten

Ergänzend zum Terminplan Jahresabschluss 2012 hat die IC Zentrale eine Anleitung zur Aktivierung 2012 erstellt. Dieses Dokument zeigt in einzelnen Schritten auf, welche Arbeiten durch die Filialen beim Ausweis der zu aktivierenden Kosten von Projekten nach deren Inbetriebnahme bzw. dem provisorischen oder definitiven Projektabschluss ausgeführt werden müssen. Im Zusammenhang mit dem Jahresabschluss hat die EFK festgestellt, dass bei der erst- bzw. zweit-Aktivierung Korrekturen vorgenommen wurden. Im Rahmen dieser Prüfung wurden bezüglich der effektiven Aktivierung beim Projektabschluss keine Prüfungshandlungen durchgeführt.

3.9 Standardisiertes Prozessvorgehen

Das FS ASTRA beinhaltet die allgemein gültigen Ablaufmodelle für die unterschiedlichen Hauptprozesse im ASTRA. Ergänzend beschreibt die IC Weisung die Prozesse im Investitionscontrolling ausführlich. Die ablauforganisatorische Ausgestaltung der Subprozesse in der IC Weisung obliegt aber, trotz umfassender Vorgaben, den einzelnen Filialen. Wie in den vorgängigen Kapiteln dargestellt, beinhaltet das FS ASTRA grundsätzlich ein gutes Vorgehen, wie die Risiken und Kontrollen abgebildet und mit dem IKS in Verbindung gebracht werden können. Grundsätzlich wäre es mit diesem Vorgehen möglich, eine einzige RKM zu erstellen, die für alle fünf Filialen Gültigkeit hat, was als effizientes Vorgehen zu beurteilen ist.

Dadurch, dass heute die Prozesse in allen Filialen unterschiedlich geregelt sind, müsste theoretisch für jede Filiale eine separate RKM erarbeitet werden, die die Risiken, die Kontrolltätigkeiten und die Vorgaben bezüglich der Kontrollnachweise pro Filiale festhält. Diese müssten dann auch noch mit den Prozessbeschreibungen in den Filialen in Verbindung gebracht werden.
Die EFK ist der Ansicht, dass dieses Vorgehen zu einer unnötigen Verkomplizierung der Dokumentation des IKS darstellt und Synergien nicht genutzt werden können.

Zudem würde es sich im Hinblick auf eine bessere technische Unterstützung oder eine allfällige Ablösung von TDcost sicherlich als wertvoll erweisen, wenn die Prozesse der Filialen bereits vorher standardisiert sind (siehe auch Kapitel 5).

Empfehlung 8 (Priorität 2):

Die EFK empfiehlt zu evaluieren, ob es nicht effizienter wäre, die Prozesse, Risiken, Kontrollen und Kontrollnachweise im FS ASTRA und in einer einzigen RKM für die Filialen verbindlich vorzugeben. Einheitliche Vorgaben würden den administrativen Aufwand im Zusammenhang mit dem IKS auf ein notwendiges Minimum beschränken. Die Prozesse in den Filialen erscheinen als ausreichend homogen, um eine einheitliche Vorgabe realisieren zu können.

Stellungnahme des ASTRA zur Empfehlung 8:
Diese Empfehlung wird mit Überarbeitung der RKM ”Einkauf Filialen (IC)” und der Vereinheitlichung des Rechnungsablaufs umgesetzt.

3.10 Gesamtbeurteilung zum IKS in den geprüften Prozessbereichen

Basierend auf den Feststellungen und Schlussfolgerungen in den einzelnen Kapiteln wird eine Gesamteinschätzung des IKS im geprüften Prozessbereich vorgenommen.

3.10.1 Prozessübergreifende Prüfungen: Bestehen Schwachstellen, die die Qualität des IKS im untersuchten Bereich tangieren?

Die Funktionentrennung im TDcost ist nicht zweckmässig und führt zu unvereinbaren Funktionskumulationen. Auf Grund der bestehenden Berechtigungen im System erscheint es durchaus als möglich, dass fiktive Rechnungen verbucht werden könnten und dass diese auch bezahlt würden. Es bestehen in diesem Bereich Kontrolllücken, die umgehend geschlossen werden müssen.

3.10.2 IKS Aufzeichnung: Ist das bestehende IKS in der Risiko- und Kontrollmatrix vollständig und richtig beschrieben?

Das IKS ist in der RKM nicht vollständig und richtig beschrieben. Insbesondere fehlen bezüglich der durchzuführenden Kontrollen sachdienliche Handlungsanweisungen. Aus der RKM geht nicht hervor, welche Kontrollen durchgeführt und wie die entsprechenden Kontrollnachweise erbracht werden müssen. Einzelne identifizierte Schlüsselrisiken sowie Kontrollen zur Risikominimierung sind in der RKM nicht aufgeführt. Bedingt dadurch, dass die Prozesse in den Filialen unterschiedlich ausgestaltet sind, müssen in den Filialen ergänzende RKM aufgebaut werden. Dieser administrative Aufwand kann allenfalls durch eine Vereinheitlichung der Prozesse in den Filialen gemindert werden.

3.10.3 IKS Design: Sind die von der Verwaltungseinheit vorgesehenen Schlüsselkontrollen angemessen und vollständig, um die Risiken einer falschen Angabe in der Jahresrechnung abzudecken?

Im Rahmen der durchgeführten Prüfung wurden durch die EFK verschiedene Schlüsselkontrollen identifiziert, die in der RKM nicht enthalten sind und auch nicht durchgeführt werden. Somit werden einzelne Risiken nicht ausreichend abgedeckt. Zudem bestehen durch die fehlende Funktionentrennung und die daraus resultierenden nicht vereinbaren Funktionskumulationen, die auch nicht mittels kompensierenden Kontrollen geschlossen werden, bedeutende Kontrolllücken

3.10.4 IKS Design: Gibt es Hinweise, dass die angewendeten Schlüsselkontrollen nicht effizient sind (Doppelspurigkeiten, Kontrollfrequenz, Mix automatisierte / manuelle Kontrollen)?

Dadurch, dass alle Filialen ihre Prozesse selber ausgestalten können, entstehen Ineffizienzen. Der gleiche Prozess, der bereits im FS ASTRA beschrieben ist, muss in jeder Filiale noch einmal dokumentiert werden. Zudem müssen Schlüsselkontrollen identifiziert werden und mit den Ablaufdiagrammen in Verbindung gebracht werden. Jede Filiale erledigt Tätigkeiten, die einmal strukturiert vorgegeben werden können und die grundsätzlich durch die IC Weisung bereits verbindlich vorgegeben sind.

3.10.5 Werden die Schlüsselkontrollen angewendet?

Verschiedene Schlüsselkontrollen werden nicht angewendet oder werden durch die fehlende Funktionentrennung durchbrochen.

3.10.6 Werden die durchgeführten Schlüsselkontrollen angemessen dokumentiert?

Die Durchführung der Schlüsselkontrollen ist in vielen Bereichen nicht nachvollziehbar dokumentiert. Das diesbezügliche Kontrollbewusstsein ist nicht vorhanden.

3.10.7 Ist das IKS in den geprüften Bereichen wirksam?

Nein, es bestehen signifikante Kontrolllücken, insbesondere im Bereich der Funktionentrennung. Insbesondere ist festzuhalten, dass der Genehmigungsprozess auf den Originaldokumenten in Papierform sorgfältig durchgeführt wird. Dieser wird aber durch die fehlende Funktionentrennung im System ausser Kraft gesetzt, wenn die Papierdokumente im System abgebildet werden.

3.10.8 Können wesentliche Kontrolllücken mit kompensierenden Kontrollen überbrückt werden?

Insbesondere im Bereich der fehlenden Funktionentrennung könnte mittels kompensierenden Kontrollen (Logfiles) eine bestehende Kontrolllücke deutlich reduziert werden. Diese Logfiles bestehen momentan noch nicht und sollten noch definiert werden. Die Rohdaten dazu fliessen seit Anfang 2011 täglich in das DWH ein. Durch die Auswertung dieser Daten (Statusänderungen, Mutationen) mit geeigneten Reports würden die kompensierenden Kontrollen ermöglicht.

4 Technische Aspekte von TDcost

4.1 Die IT-Anwendung TDcost

Mit der IT-Anwendung TDcost werden Projekte, welche den Ausbau/Unterhalt/Betrieb sowie die Engpassbeseitigung von Nationalstrassen betreffen, geführt und die entsprechenden Abrechnungen darüber abgewickelt. Die generelle Organisation des ASTRA ist so gestaltet, dass jedem Projekt ein Projektleiter (PL) zugewiesen ist und der sich auf sogenannte Bauherrenunterstützer (BHU) abstützt, welche wiederum den Projektfortschritt und die effektiven Arbeiten auf den einzelnen Baustellen überwachen. Die Projektleiter sind beim ASTRA angestellt, während die BHU Externe, i. d. R. Ingenieurbüros, sind.

Neue Projekte werden eröffnet, unabhängig davon, ob das Projekt realisiert wird. Dies kann damit zusammenhängen, dass während der Projektierungsphase noch Einsprachen eingehen, welche das betroffene Projekt stark verzögern oder gar verhindern können. Beim Ausbau oder der Engpass-Beseitigung können auch noch notwendige Landerwerbe dazu kommen, welche die Projektabwicklung zusätzlich verzögern. TDcost dient der korrekten Initialisierung der Projekte, da diese für die Abwicklung und richtige Verbuchung elementar ist.

Die Applikation TDcost wird seit 2008 operativ eingesetzt, seither hat sich die Funktionalität über viele verschiedene Programmänderungen und neue Releases stark verändert. Die Anwendung wird durch den Lieferanten (techdata) mit Hilfe eines Subunternehmers (TRIVADIS) gewartet und technisch betreut. Obwohl das ASTRA eigentlich nur mit dem Inhaber von TDcost einen Vertrag hat, braucht es die technische Unterstützung des Subunternehmers. Dies führt zu Abhängigkeiten zum Lieferanten wie auch zum Subunternehmer hinsichtlich personeller und auch technischer Aspekte. Für die Wartung von TDcost besteht ein separater Wartungsvertrag, welcher die offiziell gelieferten Releases umfasst. Daneben wurden jedoch noch umfangreiche Anpassungen vorgenommen, welche das ASTRA zusätzlich als eigentlicher Entwicklungsaufwand finanziert hat. Als Indikator für diesen Problembereich dient auch das Kostenverhältnis von gekauften Software-Lizenzen und bisher bezahlten Änderungswünschen. Während sich die ursprünglichen Lizenzkosten auf ca. 1,6 Millionen Schweizer Franken belief, hat das ASTRA bereits rund 4.2 Millionen Schweizer Franken an zusätzlichen Entwicklungen bezahlt, d. h. rund das vierfache der eigentlichen Software-Lizenz. Für weitergehende Erklärungen und Empfehlungen im Bereich der Software-Entwicklung und Abhängigkeiten verweisen wir zudem auf das Kapitel 4.7, Abhängigkeiten.

4.2 Architektur

TDcost ist eine Client/Server-Anwendung die auf einer Microsoft-Plattform basiert. Als Server dient ein Dual Core Intel-System, das den Microsoft Server 2005 als Plattform verwendet. Die Programmierung erfolgt auf Basis von Microsoft.net. Nach Performanceproblemen wurde das System auf eine 64-Bit Plattform migriert und ist nun deutlich schneller. Die Verfügbarkeit hatte sich im letzten Jahr verbessert, was anlässlich der drei Filialbesuche jeweils durch die Interviewpartner bestätigt wurde.

Für TDcost gibt es drei Systeme:

- Qualitätssicherungssystem (Q-System)

- Test/Abnahme, gleich wie Produktion (Datenabgleich 2x täglich)
- Produktion

Alle drei TDcost-Systeme werden durch das Bundesamt für Informatik und Telekommunikation (BIT) betrieben.

	Schlussfolgerung
●	Die EFK erachtet die Aufteilung auf die drei Systeme als sinnvoll und notwendig zur Sicherstellung einer stabilen Produktion und eines geordneten Änderungswesens.

4.2.1 Login

TDcost wird über ein Icon gestartet, das nur auf den Bundesarbeitsplätzen des ASTRA installiert wird. Damit ist ein direktes Login in TDcost möglich. Benutzername und Passwort müssen nicht speziell eingegeben werden, da die Anmeldeinformationen des lokalen Windows-Logins verwendet werden. Zusätzlich gibt es in Ausnahmefällen die Möglichkeit des Zugriffes über ein Eingabefenster (Pop-up) mit der U-Nummer als Benutzername und einem persönlichen Passwort. Der Zugriff auf TDcost entspricht dem für eine Anwendung ohne hohe Sicherheitsanforderungen.

Als Vorsystem für die Zahlungen ist diese Zugriffssicherheit auf TDcost zu schwach. Es kann heute nicht sichergestellt werden, dass der effektive Benutzer eindeutig festgestellt werden kann, da beispielsweise der erste Mitarbeitende am Morgen in TDcost einsteigt und dann jeder Kollege damit arbeiten könnte. Einzig das Windowspasswort zum Freischalten des Bildschirmschoners bietet einen minimalen Schutz.

Mit der Einführung der 2-Faktor-Authentisierung (BRB) steht künftig ein ein sicheres Authentisierungsmittel zur Verfügung. Dieses wird eine höhere Sicherheit durch die klare Identifikation der Benutzer bieten. Durch den persönlichen Aufwand zum Erhalt einer Smartcard wird das Sicherheitsbewusstsein der Mitarbeitenden gestärkt werden und somit ein Gruppenzugriff auf TDcost über ein Account weniger wahrscheinlich. Mit der 2-Faktor-Authentisierung könnte ein sicheres Single Sign On (SSO) umgesetzt werden, das ein automatisches Login in TDcost ermöglichen würde. Ob und zu welchen Konditionen TDcost entsprechend angepasst werden könnte, sollte abgeklärt werden. Die Zugriffe auf SAP werden in der Bundesverwaltung mit der 2-Faktor-Authentisierung abgesichert werden.

	Schlussfolgerung
■	Der heutige Zugriff auf TDcost über das Windowslogin ist schwach gesichert. Zur Erhöhung der Zugriffssicherheit sollte eine starke Authentisierung eingeführt werden. Gruppenzugriffe[7] über angemeldete PCs unterlaufen das Berechtigungssystem von TDcost.

[7] Gruppenzugriff bedeutet, dass eine Person sich in einem System anmeldet und anschliessend verschiedene Personen unter dem gleichen User arbeiten.

Empfehlung 9 (Priorität 2):

Die EFK empfiehlt, dass TDcost mit einer 2-Faktor-Authentisierung abgesichert wird, sobald diese verfügbar wird. Bis dahin ist durch Informationen und Kontrollen sicherzustellen, dass nicht mehrere Personen über denselben angemeldeten Benutzer auf TDcost zugreifen.

Stellungnahme des ASTRA zur Empfehlung 9:
Die 2-Faktor Authentisierung wird im ASTRA generell und damit auch in Bezug auf TDcost per Anfang 2014 umgesetzt.

4.2.2 Performance

Obwohl sich die Verfügbarkeit nach Aussage verschiedener Benutzer in den besuchten Filialen und in der Zentrale sehr verbessert hat, gab es im 4. Quartal 2012 ein Problem. Es traten über 300 Mal Deadlock-Situationen auf.

Deadlock‘s entstehen, wenn gleichzeitig mehrere Programme eine Tabelle öffnen wollen, die schon reserviert ist. Dadurch können die Programme nicht abgearbeitet werden und blockieren ihrerseits andere Programme. Es ist wie wenn an einer Kreuzung mit gleichberechtigten Strassen jeweils ein Auto steht und niemand weiss, wer nun Vorfahrt hat. Diese Situation kann nur durch eine Regelung (Polizist, Ampel, Kreisel oder Handzeichen) gelöst werden. Bei wenig Verkehr greift der Rechtsvortritt. Bei einem Datenbanksystem können solche Situationen immer wieder entstehen. Unter dem Jahr geschieht dies selten (3 bis 4 Mal). Für den Benutzer wirkt sich dies mit ungewöhnlich langen Antwortzeiten oder mit der Notwendigkeit von einem Neustart der Anwendung aus.

Die Vorfälle wurden durch die Firma techdata abgeklärt. Letztlich wurde jedoch nicht klar, was der Grund für diese Anhäufung war. Die Situation auf dem Q-System durch einen Lasttest nachzuvollziehen ist aus Sicht der EFK technisch kaum möglich. Als Massnahme wurde daher ein Update und Ausbau der technischen Plattform im BIT geplant. Dieser soll in den kommenden Monaten durchgeführt werden.

Für die EFK ist es plausibel, dass viele Benutzer noch vor Jahresende möglichst viel abrechnen und bezahlen wollen. Die Belastung von TDcost in dieser Zeit wird jedes Jahr sehr hoch sein. Ein möglicher Grund für die Deadlocks könnte die Kontrolle der Schwellenwerte (siehe Kapitel 3.3.2 Automatische Kontrollen) sein. Diese ist durch die vielen Regeln komplex und reserviert jeweils viele Tabellen der Datenbank. Jede Kontrolle benötigt zudem hohe Rechenleistungen und generiert viele Input und Output-Transaktionen (IO) auf der Datenbank. Die Beseitigung der Blockade braucht jeweils viel Zeit, Eingriffe ins System und ist für die Mitarbeitenden sehr ärgerlich.

Unerwarteter Weise traten nach Aussage der Leiterin IC kurz nach der Revision vor Ort wieder Deadlocks auf. Dies in einer eher ruhigen Zeit. Das ASTRA wird nun mit einer Task Force gemeinsam mit dem BIT die Ursachen untersuchen.

	Schlussfolgerung
■	Mit dem zu erwartenden zusätzlichen Aufwand aus dem Netzbeschluss (NEB) für die Übernahme von weiteren 400 km Nationalstrasse und der damit verbundenen Zunahme an Projekten, Rechnungen und Zugriffen besteht hier weiterhin ein latentes Risiko, dass TDcost der Belastung nicht standhalten könnte. Ob der Hardware- und Betriebssoftware-Ausbau die erhoffte Wirkung erzielt, wird sich erst weisen. Sollte die kürzlich gebildete Task Force die Ursachen für die schlechte Performance nicht feststellen und das Problem weiter bestehen, wird dies zu einer kritischen Schwachstelle von TDcost.

4.3 Datawarehouse

4.3.1 Das Reporting in TDcost war kostenintensiv

Das ASTRA hat verschiedene Reportingbedürfnisse zu TDcost. Bisher musste es jeweils für jede Auswertung einen Auftrag an die Firma techdata erteilen, was mit hohen Kosten und manchmal langen Lieferfristen verbunden war. Als Lösung dieses Mangels wurde ein Datawarehouse (DWH) erstellt. Da der Lieferant die Offenlegung des Datenmodells verweigerte, musste das ASTRA diese Grundlagen langwierig selbst erarbeiten. Durch die vielen Tests in den letzten 2 Jahren geht das ASTRA mittlerweile von einer guten Qualität des DWH aus.

Die Umsetzung des DWH dauerte zwei Jahre und verlief nicht ohne Probleme. Das DWH wird vom MISTRA-Team betrieben.

Das DWH fungiert als Reportingtool für ein Management Informationssystem (MIS). Das Reporting ist noch im Ausbau. Es gibt eine Liste von weiteren Anforderungen (Reporting und Controlling). Diese wird periodisch durch das IC beurteilt und nach Prioritäten umgesetzt.

Das DWH unterstützt die externen BHU noch nicht direkt, sondern nur die Mitarbeitenden des ASTRA. Diese geben die gewünschten Informationen weiterhin per Papier an die BHU weiter.

	Schlussfolgerung
■	Obwohl die Reports des DWH ausführlich getestet wurden, kann nicht vollständig ausgeschlossen werden, dass das rekonstruierte Datenmodell fehlerlos ist und alle Daten fehlerfrei sind. Die effektiven Verknüpfungen des Datenmodels sind weiterhin das Geschäftsgeheimnis von techdata. Für eine Applikation, welche im Auftrag des ASTRA für viel Geld weiterentwickelt wurde, ist es für die EFK nicht nachvollziehbar, dass die entsprechenden Informationen nicht an den Besteller übergehen. Nur eine Lösung durch den Lieferanten von TDcost könnte die Güte der Inhalte garantieren.

4.3.2 Eine Historisierung der Transaktionen wurde bisher in TDcost nicht eingesetzt

Die Anwendung TDcost des ASTRA kann die Historisierung der Abläufe nicht sicherstellen. Sie hält jeweils den Status der Erfassung der verschiedenen Daten wie Projekte, Kredite, Verträge,

Voranschlagskredite und Rechnungen mittels Angabe des letztmutierenden Benutzers in Form von User-Identifikation und Datum/Zeit fest. Wenn Anpassungen an den Daten in Form von Mutationen oder Änderungen von Stati erfolgen, wird jeweils die Kennung des letzten Benutzers eingetragen. Ein vollständiges Logging oder Journal aller Mutationen gibt es bisher nicht. Es werden keine Nachweise über zwischenzeitliche Änderungen, z. B. in Form von Mutationsjournalen, geführt.

Da das ASTRA bisher davon ausging, dass die Historisierung in TDcost nicht möglich ist, wurde ein DWH unter dem Namen Datastore aufgebaut. Seit Anfang 2011 fliessen täglich Daten aus TDcost ins DWH. Die Auswertungen der Logdaten (Statusänderungen, Mutationen, ect.) aus TDcost müsste nun im DWH programmiert werden, damit schliesslich regelmässige Kontrollen möglich werden.

	Schlussfolgerung
■	Die fehlende Historisierung in TDcost ist eine Schwachstelle, die mit dem DWH teilweise kompensiert werden konnte. Die EFK erachtet es als unabdingbar, dass ein Vorsystem zu SAP wie TDcost, das eigentlich durch die Erfassung von Rechnungen ein Teil des Buchhaltungssystems darstellt, Mutationsjournale und Nachweise von wichtigen Datenänderungen in Form eines Logging mit entsprechenden Auswertungsmöglichkeiten sicherstellt.

Empfehlung 10 (Priorität 1):

Die EFK empfiehlt, im TDcost die Funktion zur Erstellung von Mutationsjournalen und Logging aller Datenerfassungen und –änderungen sicherzustellen und die entsprechenden Auswertungen periodisch zu analysieren und nachweisbar zu kontrollieren. Diese Kontrolle könnte dann auch als kompensierende Kontrolle bezüglich der fehlenden Funktionentrennung eingesetzt werden. Bei der Umsetzung des Logging der finanzrelevanten Prozessschritte von TDcost muss der Einfluss auf die Performance in der Kapazitätsplanung beachtet und die Infrastruktur möglicherweise aufgestockt werden.

Stellungnahme des ASTRA zur Empfehlung 10:

Die Datenerfassung und -mutationen werden bereits heute im Datastore historisiert. Um Auswertungen erstellen zu können, ist der Aufbau eines Universums auf dem Datastore erforderlich. Die entsprechenden Anforderungen sind bereits definiert. Die Realisierung des Instruments erfolgt 2014.

4.4 Generelle IT-Kontrollen (ITGC)

Die ITGC wurden nach dem Schweizer Prüfungsstandard PS 890 aus der Sicht des Leistungsbezügers, Eigentümers und Auftraggebers von TDcost geprüft. Dabei wurde in den Filialen ein reduzierter Fragenkatalog mit den Themen IT-Support, lokale Infrastrukturen und IT-Sicherheit verwendet.

Folgende Feststellungen und Erkenntnisse haben sich ergeben:

4.4.1 Kontrollumgebung

- Die IT-Organisation von TDcost im ASTRA deckt die Aspekte wie folgt ab: Die Anwendungsverantwortung (AV) für TDcost liegt beim Investitionscontrolling (IC). Das Integrationsmanagement Informatik (IMI) ist für die SLA mit dem BIT sowie für das Helpdesk und die Informatik von MISTRA für den Betrieb des DWH verantwortlich.
- Es erfolgt keine Berichterstattung aus SLA an das IC. Es gibt nur gelegentliche Berichte von der Leiterin IC an die TDcost-Benutzter (letzter vom 1.4.2012). Bei Störungen wird sie, als Teil der Supportstruktur, sofort informiert.
- Die Schulung erfolgt nach Bedarf (ca. 1x/Jahr)
- Für die Beurteilung der IT-Lösungen bei den Weiterentwicklungen von TDcost und die Auftragsvergabe muss das IT-Wissen (2nd Opinion) jeweils extern eingeholt werden.
- Ein ISDS für TDcost wurde nicht erstellt (siehe Kapitel 4.6, IT-Sicherheit).

4.4.2 IT-Betrieb

- Der Betrieb von TDcost ist ans BIT delegiert
- Die Leistungen sind in einem SLA festgelegt
- Nach Aussage verschiedener Gesprächspartner in den besuchten Filialen läuft der Betrieb inzwischen stabiler

4.4.3 Incident Management und Support

- Die Support- und Eskalationsstrukturen sind bekannt (Superuser, 1st-Level-Support, Helpdesk ASTRA, IC-Zentrale/Leiterin IC für TDcost) und funktionieren.
- Die Termineinhaltung bei techdata/Trivadis sei laut Aussage des IC oft mangelhaft.
- Eskalationen gehen bei Bedarf bis zum Leiter Abt. I (Strasseninfrastruktur), d. h. das Kader engagiert sich für die Aspekte der Informatik.

4.4.4 Backup und Desaster Recovery

- Dies ist ans BIT ausgelagert und im SLA vereinbart.
- Eine Neuinstallation von TDcost wäre sehr aufwändig, da auf der ersten Installation alle Updates nachinstalliert werden müssen. Es gibt keine aktuelle Vollversion für das ASTRA.
- Das ASTRA verfügt nicht über den aktuellen Source-Code.

4.4.5 Change Management

- Das ASTRA ist Auftraggeber. Die Entwicklung ist Sache der Lieferanten. Häufig erfolgt die Projektleitung durch die Firma techdata. Die Schulung erfolgt in der Regel über das ASTRA.
- Änderungen basieren auf einem Auftrag im Change Management-Tool CMS von techdata. Die Umsetzungen erfolgen durch die Firma TRIVADIS.
- Als Grundlage für die Aufträge werden Systemdesigns erstellt. Dies sind angepasste Printscreens, welche die geplanten Auswirkungen auf die Eingabemasken aufzeigen. Diese ermöglichen eine einfache Einbindung und Präzisierung der Kundenanforderungen.

- Das ASTRA erteilt jeweils Entwicklungsaufträge, die auf Offerten von techdata basieren (Umfang, Kosten). Die Auftragserteilung muss im Rahmen des vorgesehenen Budgets erfolgen und berücksichtigt zudem Aspekte wie Dringlichkeit und Wirtschaftlichkeit.
- Grundsätzlich haben die Entwickler nur Zugriffe auf das Q-System. Begründete Ausnahmen kann das ASTRA ermöglichen.
- Tests erfolgen bei den Entwicklern von TRIVADIS (Programmtest), bei techdata (Einbindung in TDcost), beim BIT (Systemintegration) und beim ASTRA (Funktionalität).
- Bei grösseren Changes gibt es ein Abnahmeprotokoll. Für Test und Abnahme steht ein spezielles TDcost-System zur Verfügung.
- Die Leiterin IC wird über die Entwicklungen jeweils zeitgerecht informiert (CC Mail).
- Die Zusammenarbeit der Entwickler mit dem BIT sei gut.
- Nach Aussage der Leiterin IC funktioniert der Change Prozess gut.

4.4.6 Benutzer- und Zugriffsverwaltung (Access Management)

Es gibt einen geregelten Prozess für die Zuweisung von Berechtigungen auf den benötigten Systemen bei Neuanstellungen, Funktionswechsel und Austritt. Dieser funktioniert im ASTRA einheitlich. Die Berechtigungen von TDcost und SAP wurden von der EFK geprüft (siehe Kapitel 4.5, Berechtigungen).

4.4.7 Physischer Zutritt (Physical Access)

Die Gebäude des ASTRA sind mit Badges und Alarmsystemen ausgerüstet, was die EFK anlässlich der Filialbesuche verifizieren konnte. Das ASTRA verlässt sich auf die Sicherheit im Rechenzentrum des BIT.

4.4.8 Service Level Management

- Es gibt ein SLA mit dem BIT und Verträge mit techdata. Die SLA werden vom Integrationsmanager ASTRA (IMI) abgeschlossen und erneuert. Das SLA-Reporting des BIT erfolgt zu IMI. Das IC wird in der Regel nicht weiter informiert.
- Die Verträge mit techdata werden durch das IC-Zentrale erstellt.
- Wegen der oft umstrittenen versteckten Mängel wird die Gewährleistung im neuen Vertrag mit techdata auf 18 Monate erhöht.

	Schlussfolgerung
●	Die generellen IT-Kontrollen im Umfeld von TDcost liegen mit Ausnahme der Applikationsentwicklung beim BIT. Die Qualität der Betriebsprozesse wird in den SLA oder Verträgen festgelegt. Die Dienstleistungen des BIT werden vom IC als gut und solide wahrgenommen. Die besuchten Filialen bestätigten die verbesserte Verfügbarkeit von TDcost. Die Prüfung der ITGC im BIT erfolgt in einer separaten Revision.

4.5 Berechtigungen

4.5.1 Die Berechtigungen von TDcost

Zur Prüfung der Berechtigungen von TDcost diente die TDcost-Benutzerliste mit der Rollenzuteilung aus dem produktiven System (Download vom 27.05.2013). Die Daten wurden in Anwesenheit der EFK direkt aus dem produktiven System extrahiert.

Folgende Punkte sind wichtig:

- Die Aussagen sind nur für die Momentaufnahme (27.05.2013) der Datenextraktion gültig.
- Jeder TDcost-Benutzer hat nur eine Rolle zugeteilt. Der Benutzername ist wie bei SAP die U-Nummer.
- Das Berechtigungssystem in TDcost kennt 132 Funktionen wie beispielsweise *AuswertungProjektaddresse*, *ZahlungskreditMutationen* oder *RechnungGenehmigung*. Auf diesen gibt es die Rechte Ausführen/Lesen, Erstellen, Ändern und Löschen. Da nicht, wie in SAP, einzelne Transaktionen mit speziellen Ausprägungen über die Berechtigungen gesteuert werden können, sichert das Berechtigungssystem in TDcost vor allem die wichtigen Funktionen.
- Da die Dokumente in FABASOFT nur verlinkt sind, gelten implizit die Rechte von TDcost.
- Externe Mitarbeitende haben keine Berechtigungen auf Management Informationen (MIS), auf Kataloge oder Adressen. Es fehlt selbst das Menu zum Aufruf, somit stehen die Funktionen nicht zur Verfügung.
- Die Berechtigungen wurden formal gemäss Anhang 5 zur IC-Weisung Teil C (Stand 05.09.2012) umgesetzt. Dabei ist es eine andere Frage, ob das Design des Berechtigungskonzepts den Anforderungen wirklich genügt. Der Bereichsleiter IC (I-IC) und die Leiterin IC verfügen über die Rolle ADMIN. Dies bedeutet sie haben alle Rechte (analog SAP_ALL).
- Die Leiterin IC ist operativ die Stellvertreterin vom Bereichsleiter IC (I-IC) und hat gleichzeitig administrative Aufgaben. Beispielsweise werden die privilegierten Rollen (hohe Rechte) nur durch sie zugeteilt. Ihrerseits bestehen nur punktuelle Stellvertretungen.
- Die Analyse zeigt, dass die zugeteilten Berechtigungen in den Filialen wenig einschränken. Es werden nur wenige Rechte selektiv vergeben. Dies sei laut IC so gewollt, da somit in der kritischen Zeit Ende Jahr, möglichst viele Mitarbeitende bei der Bearbeitung der Rechnungen mithelfen können.
- Der Fakturaprozess wird über die Trennung von Filiale und Zentrale abgesichert. Die Rechnungsfreigabe erfolgt nur in der Zentrale. Diese kann jedoch die Richtigkeit der Rechnungen nur stichprobenweise kontrollieren. Damit wirkt diese Trennung nicht im Sinne einer Funktionentrennung.

	Schlussfolgerung
▲	Die EFK kommt nach Analyse der Berechtigungen von TDcost zum Schluss, dass das Berechtigungskonzept des Anhangs 5 zur IC-Weisung Teil C (Stand 05.09.2012) in TDcost formal korrekt umgesetzt wurde. Sie genügen jedoch nicht den Anforderungen einer wirksamen Funktionentrennung. Die Filialen sind nach der Weisung organisiert und haben die Rollen den Funktionsträgern analog deren Funktion zugeteilt. Die Prüfung der einzelnen Rollen konzentrierte sich auf die statusverändernden Berechtigungen. Verschiedene Rollen in den Filialen unterscheiden sich nur wenig. Die Qualität der Abwicklung des Kredito-

	renprozesses wird von IC durch die Prüfung von Stichproben verifiziert. Die materiellen Kontrollen müssen jedoch in den Filialen erfolgen. Die Zentrale und der Finanzdienst, welche die Zahlungen letztlich auslösen, können nur formale Kontrollen durchführen. Aus Sicht des Rechnungsprozesses muss eine straffere Berechtigungssteuerung umgesetzt werden.

Empfehlung 11 (Priorität 1):

Die EFK empfiehlt, dass das Berechtigungskonzept den effektiven Kontrollmöglichkeiten angepasst werden muss und die Funktionentrennungen so gestaltet werden, dass das 4-Augenprinzip zwingend eingehalten wird, da heute die Zahlungsfreigabe eigentlich – bis auf die stichprobenweise Plausibilisierung von einzelnen Rechnungen – schon in der Filiale mit der Genehmigung erfolgt. Die Verantwortung muss klar bei den Filialen liegen und auch so definiert werden.

Stellungnahme des ASTRA zur Empfehlung 11:
Die Berechtigungen in TDcost werden so angepasst, dass das 4-Augen-Prinzip in den Filialen bei der Prüfung und Freigabe der Zahlungen umgesetzt wird. Die Stichprobenkontrollen in der Zentrale werden beibehalten.

4.5.2 Die Berechtigungen von SAP

Die EFK hat eine Berechtigungsprüfung des SAP-Systems (NRM) durchgeführt.

Die Auswertung der Rollenzuteilungen und der Logindaten (Mandant 610) hat ergeben:

- An 255 Mitarbeitende des ASTRA wurden 174 verschiedene Profile zugeteilt.
- 75 Profile enthalten die Berechtigung anzeigen und werden als unkritisch eingestuft (grün).
- 99 Profile enthalten pflegen oder andere Mutations-Rechte (gelb).
- Davon sind mindestens 6 sehr kritische Berechtigungen (rot).
- Von den 255 Mitarbeitenden mit SAP-Rechten verfügen 62 über kritische Rechte. Diese ist plausibel, da die Meisten davon in der Finanzbuchhaltung (und im Controlling) arbeiten.
- Es haben keine Mitarbeitende der IC-Zentrale Berechtigungen im Bereich Finanzen (RFI-Profile). Die Leiterin IC verfügt als einzige über Leserechte.
- Die Zahlungsfreigabe (Zahllauf) wurde nur an 4 Personen in der Finanzbuchhaltung ASTRA zugeteilt.
- Von den Filialen haben keine Mitarbeitenden Rechte im SAP (RFI).

	Schlussfolgerung
●	Die Berechtigungen im SAP sind in Bezug auf die Bezahlung der Rechnungen aus TDcost so zugeteilt, dass es keine Vermischung zwischen den Aufgaben des IC der Zentrale und der Finanzbuchhaltung des ASTRA gibt. Die Freigabe der Zahlungen in SAP erfolgt nur aufgrund formeller Kontrollen. Die Rechnung ist in TDcost und kann von der Finanzbuchhaltung nicht weiter überprüft werden. Bei Fehlern geht diese zurück an das IC.

4.6 IT-Sicherheit

Für TDcost wurde im Juli 2012 durch das ASTRA eine Schutzbedarfsanalyse erstellt. Dabei wurde kein erhöhter Schutzbedarf festgestellt und der Grundschutz als genügend definiert. Ein ISDS (Informationssicherheit- und Datenschutzkonzept) für TDcost wurde als nicht notwendig beurteilt. In Anbetracht der Sensibilität einzelner Informationen (Kreditoren, Verträge, Rechnungen) in TDcost und im DWH ist die EFK mit dieser Einschätzung nicht einverstanden. Aus Sicht der EFK muss der Schutzbedarf nochmals evaluiert und ein ISDS erstellt werden.

	Schlussfolgerung
■	Der ursprünglich identifizierte Grundschutzbedarf der Daten von TDcost ist aus der aktuellen Sicht nicht ausreichend. Der Schutzbedarf sollte nochmals mit einem ISDS evaluiert werden.

Empfehlung 12 (Priorität 2):

Die EFK empfiehlt, in Anbetracht der Sensibilität einzelner Informationen (Kreditoren, Verträge, Rechnungen) in TDcost und im DWH, den Schutzbedarf nochmals zu evaluieren und ein ISDS zu erstellen.

Stellungnahme des ASTRA zur Empfehlung 12:

Das ASTRA wird den Schutzbedarf nochmals evaluieren und ein ISDS erstellen.

4.7 Abhängigkeiten

4.7.1 Intern

Die Leiterin IC hat ein umfassendes Wissen und viel Erfahrung zu allen Aspekten um TDcost. Eine Stellvertretung ist nur punktuell gegeben. Die fachlichen Themen können durch den Bereichsleiter IC (I-IC) abgedeckt werden, jedoch werden die eher technischen Aufgaben bei Abwesenheit der Leiterin IC nicht genügend abgedeckt. Neben der Funktion als Anwendungsverantwortliche TDcost (Support, Auftragsvergabe, Test und Abnahme) hat die Leiterin IC mit ihrem Team auch operative Aufgaben. Diese breite Palette kann, im Stellvertretungsfall nur über mehrere Personen abgedeckt werden. Ein längerer Ausfall oder Weggang wäre für das ASTRA ein erhebliches Problem.

4.7.2 Extern

Eine externe Abhängigkeit besteht primär von den Lieferanten *techdata* und *TRIVADIS Basel*. Da die Anwendung durch den Inhaber (techdata) mit Hilfe eines Subunternehmers (TRIVADIS) gewartet, weiterentwickelt und technisch betreut wird, bestehen massgebliche Abhängigkeiten zu diesen Parteien. Das Wissen über TDcost ist bei techdata und bei TRIVADIS auf wenige Personen verteilt. Einen ernsthaften Ausfall des Architekten von TDcost bei techdata könnte das Ende der Weiterentwicklung von TDcost bedeuten. Für techdata ist TDcost nur ein kleiner Geschäftsbereich, das Hauptgeschäft liegt in der Bauherrenunterstützung (BHU) und Projektleitung. Das ASTRA hat die

Firma techdata mit mehreren Aufträgen in diesen Bereichen bedacht. Zur Sicherung des Wissens von techdata und TRIVADIS schliesst das ASTRA extra Wartungsverträge ab. Das ASTRA hat wegen der Abhängigkeit bei TDcost wenig Einfluss auf die Preise für die Weiterentwicklung oder Änderungen.

Als sehr problematisch ist auch die Tatsache einzustufen, dass Mitarbeiter der Firma techdata in den TDcost-Systemen des ASTRA aus Supportgründen, Rollen zugeteilt haben und Daten einsehen können. Auch auf der Produktion haben diese Leserechte (Rolle INFO). Da die Firma techdata auch andere Aufträge vom ASTRA erhalten hat, beispielsweise in MISTRA oder als BHU, kann dies eine Bevorteilung gegenüber den andern Anbietern bedeuten. Mit den Leserechten können die Mitarbeiter der Firma techdata beispielsweise die Kostenvoranschläge und damit sowohl die Volumina, wie auch die Umsätze der Konkurrenz einsehen und diese Informationen bei den eigenen Offerten berücksichtigen (Insiderwissen). Das Problem kann mit einer Sperrung der Leserechte auf der Produktion nicht gelöst werden, da die Daten auf den anderen Systemen, nur etwas Zeitverschoben, denen der Produktion entsprechen. Nach Tests vom ASTRA ist es zumindest nicht möglich die in FABASOFT verlinkten Dokumente zu sehen. Das Dilemma kann aus Sicht TDcost nicht einfach gelöst werden. Konsequenterweise müsste techdata entweder Lieferant von TDcost oder Dienstleistungserbringer für das ASTRA sein. Beides gleichzeitig ist nicht möglich.

	Schlussfolgerung
▲	Die internen und externen Abhängigkeiten sind sehr gross. Die Zuspitzung auf einzelne Wissensträger verschärft die Problematik. Die Abhängigkeit von einzelnen Personen bei den Lieferanten ist mittel- und langfristig ein Risiko. Es muss sichergestellt werden, dass das Wissen im ASTRA erhalten bleibt, solange TDcost im Einsatz steht. Die Dreiecksbeziehung ASTRA-techdata-TRIVADIS macht den Support und die Weiterentwicklung von TDcost kostenintensiv.

Empfehlung 13 (Priorität 2):

Die EFK empfiehlt, zur Sicherung des internen Wissens sicherzustellen, dass die bestehenden Dokumente wie Systembeschreibungen, Handbücher, Entwicklungsaufträge, Verträge und SLA, Abnahmeprotokolle, Berichte, Pendenzenlisten, Sitzungsprotokolle etc. in einer strukturierten und aktualisierten Ablage für die Stellvertretenden zugänglich gemacht werden. Diese Ablage sollte regelmässig kontrolliert und aktualisiert werden.

Stellungnahme des ASTRA zur Empfehlung 13:

”Zentrale Dokumente wie Verträge und SLA sind bereits heute im GEVER ASTRA abgelegt.

Andere, heute auf der Projektplattform abgelegten Dokumente, die nicht (mehr) bewirtschaftet werden, werden ins GEVER ASTRA überführt.

Bewirtschaftete Dokumente bleiben gemäss Weisung Schriftgutplan der Abteilung Strasseninfrastruktur auf der Projektplattform.”

4.8 TDcost ist kostenintensiv, da es für das ASTRA zu einer Individualanwendung ausgebaut wurde

TDcost wurde ursprünglich als Hilfsmittel und Vorsystem für die Projektleiter erstellt. Es unterstützte die Kostenkontrolle (Investitionskontrolle) und die laufende Entwicklung des Projektes. Das ASTRA hat auf diesem Werkzeug die komplexe Struktur mit den Filialen und den verschiedenen Finanzierungselementen und Krediten aufgebaut. Heute dient TDcost als Vorsystem der Buchhaltung des Bundes (SAP/NRM) zur Zahlung der Rechnungen aus den Projekten. Diese Erweiterungen zeigen sich auch in den Kosten. Während sich die ursprünglichen Beschaffungskosten (Lizenz) auf ca. 1,6 Millionen Schweizer Franken beliefen, hat das ASTRA bisher rund 4.2 Millionen Schweizer Franken an zusätzlichen Entwicklungen bezahlt. Damit wurde aus dem Standardprodukt TDcost eine Individuallösung des ASTRA. Für die Wartung von TDcost besteht ein separater Wartungsvertrag, der die offiziell gelieferten Releases der Basisteile (Standardprodukt) umfasst.

Die Weiterentwicklung ist kostenintensiv, da bei technischen Abklärungen von Erweiterungen und Änderungen der Inhaber von TDcost (Firma techdata) meist noch die technische Unterstützung des Subunternehmers (TRIVADIS) braucht. Dies gilt für die Abklärungen, die Offerten und letztlich für Test und Abnahme. Diese Dreiecksbeziehung ist schon aus der Struktur heraus kostenintensiv und schränkt das ASTRA bei den Preisen stark ein, da es für die Weiterentwicklung keine Alternativen gibt.

	Schlussfolgerung
▲	Der Source-Code von TDcost ist beim ASTRA nicht gesichert. Dies sollte jedoch bei der Firma techdata verlangt werden. Möglicherweise könnte das ASTRA die Basiselemente von TDcost der Firma techdata abkaufen und wäre somit im Besitze des Datenmodells. Dies könnte mehr Markt und eigenes Wissen in Weiterentwicklung bringen und somit zu günstigeren Lösungen führen.

Empfehlung 14 (Priorität 2):

Die EFK empfiehlt, zur Sicherung der Anwendung TDcost, den Source Code des jeweils aktuellen Releases sicherzustellen. Es ist zu Verhandeln, ob der Code dem ASTRA ausgehändigt oder ob dieser bei einem unabhängigen Dritten hinterlegt werden soll.

Stellungnahme des ASTRA zur Empfehlung 14:

Das ASTRA nimmt Anfang 2014 Gespräche mit dem BIT über ein zentrales Source Code Management auf. Sobald die entsprechenden Vorgaben formuliert sind, wird das ASTRA mit techdata entsprechende Verhandlungen aufnehmen.

5 TDcost genügt den Anforderungen eines Finanzsystemes nur teilweise

Der ursprüngliche Zweck von TDcost war die Unterstützung der Projektleiter für das Controlling der laufenden Projekte. Das ASTRA verwendet TDcost als erweitertes Controlling-Werkzeug für die Kostensteuerung der Projekte in den Filialen mit den Detailaspekten wie Kostenvoranschlag (KV), Voranschlagskredit (VAK) und Verträge und als Vorsystem für die Abwicklung von Fakturen. Das eigentliche Zahlungs- und Buchhaltungssystem ist SAP. Die Prüfung hat ergeben, dass das System TDcost nicht über die Qualitäten, die an ein finanzrelevantes System gestellt werden verfügt. Es wurde nicht dafür entwickelt. Die Anforderungen an die Datensicherheit, die Belegsicherheit, die Journalisierung und das IKS sind zu wenig ausgebaut. Andere wichtige Funktionen zur Unterstützung der Projektleiter und Filialen, wie beispielsweise die Kontrolle der Termine von Rechnungen im Prüfprozess werden nicht in TDcost, sondern weiterhin mit Excel überwacht.

Die nötigen Investitionen um die Anforderungen die im Bericht aufgezeigt werden zu erfüllen bedeuten einen hohen Aufwand. Künftige Änderungen und Anpassungen würden auf einer Speziallösung des ASTRA und nicht in einem Standard aufbauen.Zudem ist es fraglich, ob beispielsweise die Umsetzung der E-Rechnung und deren automatisierte Bearbeitung in TDcost, möglich werden. Auch die Umsetzung des einheitlichen „Vertragsmanagement Bundesverwaltung“ und des elektronischen Kreditorenworkflows scheint aus heutiger Sicht nicht realisierbar oder würde vermutlich massive Kosten verursachen. Die zeitweise auftretenden Performanceprobleme mit den häufigen Deadlooks deuten auf eine unsichere (fehlerhafte) technische Umsetzung hin. Unter Umständen wäre es langfristig wirtschaftlicher auf ein Standardprodukt der Bundesverwaltung umzustellen.

	Schlussfolgerung
■	TDcost erfüllt die Anforderungen der Filialen an die Unterstützung der Projektleiter nur teilweise. Den Qualitätsanforderungen an ein Vorsystem des Buchhaltungssystems des Bundes, über welches Zahlungen von mehr als 1.5 Mia. Franken pro Jahr abgewickelt werden, genügt TDcost nicht. Es gibt interne und externe Abhängigkeiten, die grosse Risiken beinhalten und hohe Kosten verursachen. Diese Mängel erfordern mittelfristig bessere Lösungen, was möglicherweise die Ablösung von TDcost zur Folge haben könnte.

Empfehlung 15 (Priorität 1):

Die EFK empfiehlt zu prüfen, ob es zur Behebung aller Probleme, unter Berücksichtigung der dafür anfallenden Kosten („ein Fass ohne Boden“), vielleicht nicht sinnvoller wäre, eine andere Applikation einzusetzen. In jedem Falle wäre mit Sofortmassnahmen das bestehende IKS zu stabilisieren.

Stellungnahme des ASTRA zur Empfehlung 15:
Das ASTRA wird diese Empfehlung der EFK umsetzen und TDcost mittelfristig ablösen. Die Evaluation von Alternativlösungen wird demnächst lanciert. Dabei müssen jedoch sowohl die Bedürfnisse der Finanzbuchhaltung als auch diejenigen des Projektmanagements abgedeckt werden.

6 Schlussbesprechung

Die Schlussbesprechung fand am 23. September 2013 statt. An der Besprechung nahmen teil:

Bundesamt für Strassen
Jürg Röthlisberger, Stv. Direktor und Leiter Strasseninfrastruktur
Jean-Bernard Duchoud, Stv. Leiter Strasseninfrastruktur und Bereichsleiter Investitionscontrolling
Christian Klaus Kellerhals, Bereichsleiter Entwicklung / Stab, ab 1.10.13 BL Investitionscontrolling
Susanne Caseri, Leiterin Investitionscontrolling/Stv BL

Eidg. Finanzkontrolle
Robert Scheidegger, Mandatsleiter
Carole Balli, Revisorin
Peter Bürki, Revisionsleiter

Sie ergab grösstenteils eine Übereinstimmung mit den Feststellungen, Beurteilungen und Empfehlungen dieses Berichtes. Die EFK dankt für die gewährte Unterstützung.

EIDGENÖSSISCHE FINANZKONTROLLE

Robert Scheidegger	Peter Bürki
Mandatsleiter	Revisionsleiter

Anhang 1: Rechtsgrundlagen

Finanzkontrollgesetz (FKG, SR 614.0)
Finanzhaushaltgesetz (FHG, SR 611.0)
Finanzhaushaltverordnung (FHV, SR 611.01)
Bundesinformatikverordnung (BinfV, SR 172.010.58)

Anhang 2: Abkürzungen, Glossar, Priorisierung der Empfehlungen der EFK

Abkürzungen:

ASTRA	Bundesamt für Strassen
AV	Anwendungsverantwortliche/r
BIT	Bundesamt für Informatik und Telekommunikation
BHU	Bauherren Unterstützung
DWH	Data Warehouse
EFK	Eidg. Finanzkontrolle
FISP	Finanzinspektorat ASTRA
FS ASTRA	Führungssystem ASTRA
FSNS	Fertigstellung Nationalstrasse
IC	Investitionscontrolling
IC Weisung	Weisung zum Investitionscontrolling des ASTRA
ICNS-Tool	Investitionscontrolling Nationalstrassen Tool (Hilfsanwendung)
IF	Infrastrukturfonds
IKS	Internes Kontrollsystem
ITGC	Generelle IT-Kontrollen (Information Technology General Controls)
KV	Kostenvoranschlag
NEB	Netzbeschluss (Nationalstrassen)
NS	Nationalstrassen
PL	Projektleiter
Q-System	Qualitätssicherungssystem der Anwendung TDcost
RKM	Risiko-Kontrollmatrix
SLA	Service Level Agreement (Dienstleistungsvereinbarung)
UG	Umgestaltung Nationalstrassen
VAK	Voranschlagskredit

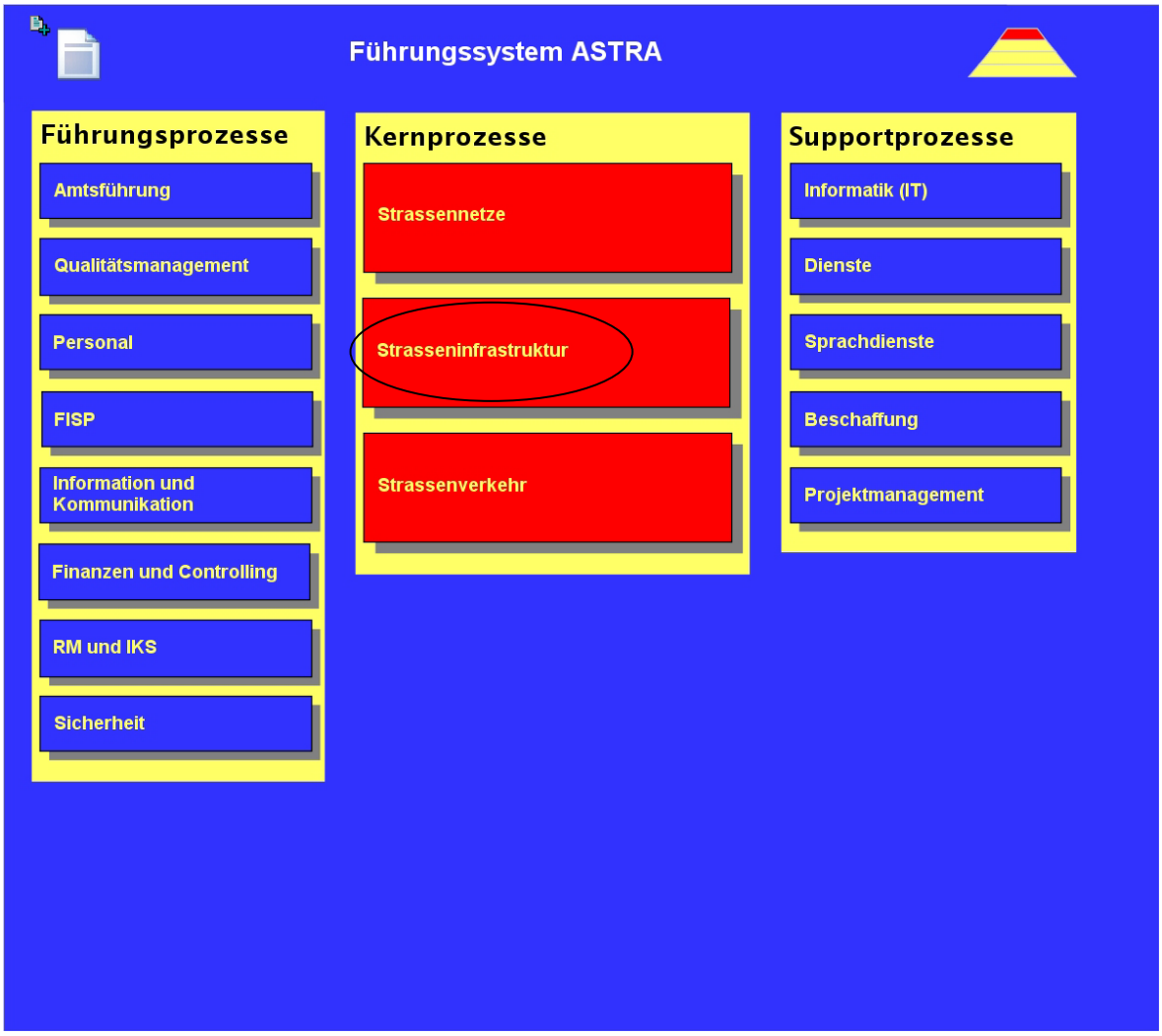
Glossar:

2-Faktor-Authentisierung	Starke Authentisierungsmethode mit einem Token - Prinzip: Etwas Wissen (Passwort) und etwas Haben (Token mit Zertifikat)
FABASOFT	Anwendung für die Dokumentenablage von TDcost
F-ICR	Name einer Berechtigungsrolle von TDcost für die Filialen
ISDS	Informationssicherheits- und Datenschutzkonzept bei erhöhtem Schutzbedarf
MISTRA	Managementinformationssystem Strasse und Strassenverkehr
NFA	Neuer Finanzausgleich (Neugestaltung des Finanzausgleichs und der Aufgabenverteilung zwischen Bund und Kantonen)
TDcost	Anwendung für das Projektmanagement (Nationalstrassenprojekte)
techdata	Lieferant der Anwendung TDcost
TRIVADIS	Subunternehmen der Firma techdata, Software-Entwickler von TDcost
WINSCP	Bezeichnung eines Schnittstellen-Servers
XML-Datei	Datei für den Datenaustausch (im Format der Extensible Markup Language)

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.

Anhang 3: Prozessabbildungen im FS ASTRA

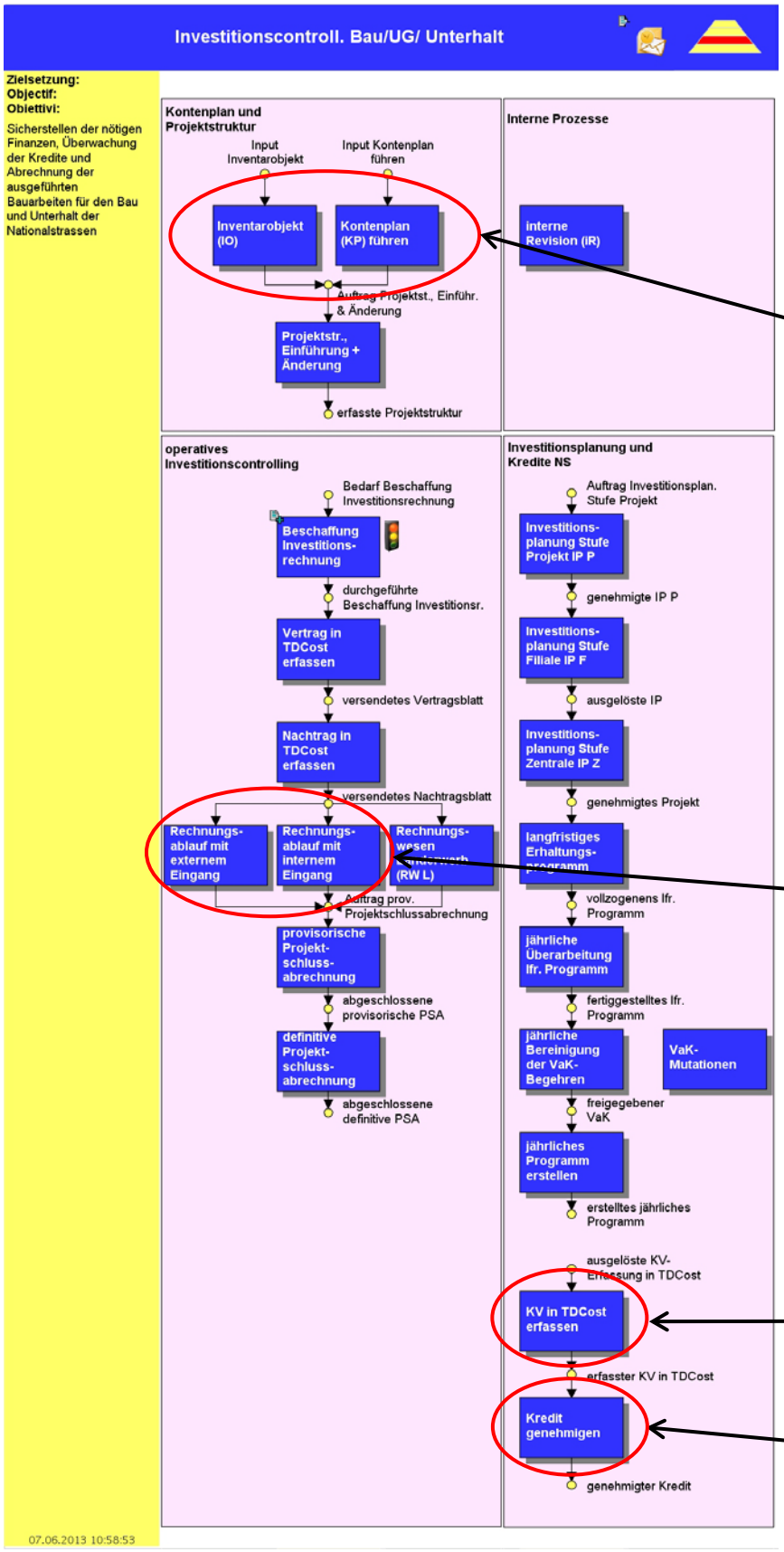
Ebene 1



Ebene 2


Strasseninfrastruktur
Zielsetzung:
Objectif:
Obiettivi:
####
07.12.2012 08:26:52
Fertigstellung des beschlossenen NS-Netzes (FSNS)
Fertigstellung NS-Netz (FSNS)
Subventio-nierung
Landerwerb FSNS
Investitions-controlling FSNS
Bau, Ausbau und Betrieb der NS
Bau und Ausbau NS
Auditmass-nahmen AB umsetzen
Projekt-gestützter Unterhalt NS
Überwachung NS
Betrieb und projektfreier Unterhalt NS
Baupolizei
Landerwerb NS
Umgang mit Schadenersatz-forderung
Investitions-controll. Bau/UG/ Unterhalt
temporäre Prozesse (für die Dauer der NFA-Einführung)
Projektüber-gabeprotokoll
temporäre Prozesse Filialen

Ebene 3



Kapitel 7.1

Kapitel 7.4

Kapitel 7.2

Kapitel 7.3