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

Prüfung der Integration der Informatik Gotthard-Basistunnel in die SBB

Bundesamt für Verkehr

EFK-16201 / inkl. Stellungnahmen / 11. August 2016

Impressum

Bestelladresse **Adresse de commande** **Indirizzo di ordinazione** **Order address**	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45, CH - 3003 Bern http://www.efk.admin.ch
Bestellnummer **Numéro de commande** **Numero di ordinazione** **Order number**	1.16201.802.00278.009
Zusätzliche Informationen **Complément d'informations** **Informazioni complementari** **Additional information**	E-Mail: info@efk.admin.ch Tel. +41 58 463 11 11
Originaltext **Texte original** **Testo originale** **Original text**	Deutsch Allemand Tedesco German
Zusammenfassung	Deutsch (« Das Wesentliche in Kürze »)

Prüfung der Integration der Informatik Gotthard-Basistunnel in die SBB
Bundesamt für Verkehr

Das Wesentliche in Kürze

Die Eidgenössische Finanzkontrolle (EFK) untersuchte die Wirksamkeit des Vorgehens zur Gewährleistung eines angemessenen IT-Sicherheitsniveaus der Tunnel-Betriebsautomation – unter Ausklammerung der Bahnleittechnik. Zudem betrachtete die EFK das methodische Vorgehen zur Durchführung der Risikoanalyse Gotthard-Basistunnel (GBT) / Ceneri-Basistunnel (CBT) sowie die konsistente Ableitung eines Massnahmenkatalogs und dessen Umsetzung. Die Kosten für die Bereitstellung der Tunnel-Leittechnik beliefen sich auf circa 50 Millionen Franken.

Die Identifikation und die Minimierung der Risiken waren zielführend, erfolgten jedoch zu spät

Am 1. Juni 2016 übergab die Erstellerin AlpTransit Gotthard AG (ATG) den GTB an die Betreiberin SBB. Aus Sicht der IT-Sicherheit waren zu diesem Zeitpunkt noch nicht alle notwendigen Massnahmen umgesetzt. Diese sollen entsprechend den ICT-Sicherheitsvorgaben der SBB fertiggestellt werden. Sorgfältig durchgeführte Analysearbeiten der SBB zeigen auf, dass zum Zeitpunkt der Betriebsaufnahme aufgrund der vorhandenen Schwachstellen keine Risiken der Einstufung „ROT“ – d. h. kurz- und mittelfristig untragbar – zu verzeichnen sind. Zudem sind die Risiken aus Sicht der ICT-Security auf den Bereich der Verfügbarkeit des Tunnels beschränkt. Auch hinsichtlich der Betriebssicherheit, etwa Unfallrisiken mit Personenschäden, hat die Analyse keine relevanten Gefährdungen festgestellt.

Während der Bauphase stellte die SBB fest, dass keine übergeordnete Sicherheitskonzeption für ICT-Security bestand. Sie erarbeitete daraufhin in Eigenregie die noch fehlende Sicherheitskonzeption „Teilkonzept (TK) übergeordnete ICT-Security GBT/CBT“. Darauf basierend untersuchte die SBB, mit Unterstützung der ATG, ob die Sicherheitsanforderungen mit der damals vertraglich vorgesehenen Umsetzung des Infrastrukturaufbaus erfüllt würden. In der Folge wurden die dabei festgestellten Schwachstellen durch die SBB aufgrund ihrer Risiken gewichtet. Es war kein Risiko der Stufe „ROT“ zu verzeichnen. ATG und die SBB verfassten einen Plan mit 42 Verbesserungsmassnahmen zur Behebung dieser Schwachstellen. Daraus entstand der Projektänderungsantrag „ICT-Security GBT“ vom 20. Mai 2014, worin die Umsetzung der Massnahmen abgedeckt war. Vor der Eröffnung des GBT überprüfte die SBB den Stand dieser Massnahmen und legte dar, dass erst 12 umgesetzt und von den verbleibenden 30 4 zurückgestellt worden waren. Im Rahmen des Anlage-Übergangs per 1. Juni 2016 sind gemäss ATG weitere Massnahmen umgesetzt worden. Diese sind zum Zeitpunkt der Berichterstellung hinsichtlich ihrer Wirkung noch nicht verifiziert.

Das Bundesamt für Verkehr ist als Aufsichtsbehörde zu stärken

Die EFK stellt fest, dass die ICT-Security-Risiken erst spät im Projekt systematisch behandelt wurden. Sie erkennt, dass die Risikoanalyse methodisch in sachgemässer Weise durchgeführt und dokumentiert ist, konstatiert aber, dass die ATG den Fortschritt der Verbesserungsmassnahmen anders beurteilt als die SBB und dass unterschiedliche Beurteilungsgrundlagen seitens der SBB und ATG angewandt werden. Aus Sicht der EFK bestehen dadurch ein Risiko zusätzlicher Kosten wie auch eine Quelle für Verzögerungen. Folglich empfiehlt sie dem Bundesamt für Verkehr (BAV), die Umsetzung der noch offenen Empfehlungen überwachen zu lassen. Ausserdem empfiehlt sie dem BAV, sowohl für den CBT als auch für weitere grosse Bahnbauprojekte mit unterschiedlichem Ersteller

und Betreiber eine Rolle beim Ersteller einzufordern, welche die ICT-Security über alle Phasen des Projektes übergreifend verantwortet und als Schnittstelle zu einer gleichartig gelagerten Rolle beim Betreiber dient. Eine solche Rolle sollte ebenso bei Vorhaben in einer Projektorganisation eingefordert werden, bei denen der Ersteller und der Betreiber die gleiche Gesellschaft sind. Sinngemäss sollte sie dann die Schnittstelle zwischen der Projekt- und der Betriebsorganisation bilden.

Contrôle de l'intégration de l'informatique du tunnel de base du Saint-Gothard chez les CFF
Office fédéral des transports

L'essentiel en bref

Le Contrôle fédéral des finances (CDF) a examiné l'efficacité de la procédure visant à garantir un niveau approprié de sécurité informatique de l'automatisation du tunnel, en excluant les systèmes de commande. Il a aussi étudié la méthodologie d'analyse des risques que présentent les tunnels de base du Saint-Gothard (TBG) ainsi que du Ceneri (TBC) et vérifié si cette analyse avait débouché sur l'élaboration d'un catalogue de mesures cohérent et sur sa mise en œuvre. Les frais de mise en place des systèmes de gestion du TBG se sont élevés à environ 50 millions de francs.

L'identification et la réduction des risques se sont avérées efficaces, mais tardives

Le 1er juin 2016, la société Alp Transit Gotthard SA (ATG) chargée de la construction a remis le TBG aux CFF qui en assureront l'exploitation. À cette date, toutes les mesures requises au niveau de la sécurité informatique n'avaient pas encore été prises. Elles devront aussi l'être selon les directives des CFF en matière de sécurité des technologies de l'information et de la communication (TIC). L'analyse réalisée avec minutie par les CFF montre qu'au moment de la mise en service, les points faibles toujours présents n'occasionnaient aucun risque de catégorie «ROUGE», c'est-à-dire inacceptable à court et à moyen terme. De plus, au niveau de la sécurité des TIC, les risques sur la disponibilité du tunnel sont limités. Enfin, l'analyse n'a révélé aucune menace importante sur la sécurité de l'exploitation, comme des risques d'accidents avec dommages corporels.

Durant la phase de construction, les CFF ont constaté qu'il n'existait pas de stratégie supérieure en matière de sécurité des TIC. Ils ont donc eux-mêmes élaboré un «concept partiel de sécurité des TIC supérieure TBG/TBC». Sur cette base, les CFF ont examiné avec le soutien d'ATG si la mise en place des infrastructures, alors prévue contractuellement, pourrait satisfaire aux exigences en la matière. Par la suite, ils ont pondéré les points faibles détectés en fonction des risques qu'ils représentent. Aucun d'eux n'était de catégorie «ROUGE». La société ATG et les CFF ont rédigé un plan de 42 mesures d'amélioration pour y remédier. Ils ont ensuite établi une demande de modification de projet «Sécurité des TIC TBG» le 20 mai 2014 pour couvrir la mise en œuvre de ces mesures. Avant l'inauguration du TBG, les CFF ont contrôlé l'état de réalisation de ces mesures et constaté que seules douze l'avaient été et que quatre des 30 mesures restantes avaient été repoussées. Dans le cadre de la remise des installations au 1er juin 2016, d'autres mesures ont été mises en œuvre au dire d'ATG. Leur effet n'a pas encore pu être vérifié au moment de la rédaction du présent rapport.

Il faut renforcer l'Office fédéral des transports comme autorité de surveillance

Le CDF constate que les risques en matière de sécurité des TIC ont été abordés tardivement de manière systématique. Il reconnaît que l'analyse des risques était méthodique, appropriée et bien documentée, mais constate qu'ATG a évalué autrement que les CFF l'avancement des mesures d'amélioration et que les deux partenaires employaient des bases d'appréciation différentes. Le CDF estime que cela risque de provoquer des coûts supplémentaires et des retards. Par conséquent, il recommande à l'Office fédéral des transports (OFT) de faire surveiller la mise en œuvre des recommandations en suspens. De plus, il lui conseille d'exiger, dans le cas du TBC ou d'autres grands projets de construction ferroviaire impliquant un constructeur et un exploitant différents, qu'un organe

chez le constructeur assume la responsabilité de la sécurité des TIC au cours de toutes les phases du projet et assure les échanges avec l'organe chargé des mêmes fonctions du côté de l'exploitant. Une telle fonction devrait aussi être imposée dans le cadre de l'organisation d'un projet, lorsque la même société en assure la construction et l'exploitation. Par analogie, cet organe devrait veiller aux échanges entre l'organisation du projet et celle de l'exploitation.

Texte original en allemand

Verifica dell'integrazione dell'informatica della galleria di base del San Gottardo nelle FFS
Ufficio federale dei trasporti

L'essenziale in breve

Il Controllo federale delle finanze (CDF) ha esaminato l'efficacia della procedura volta a garantire un livello di sicurezza IT adeguato dell'automazione dell'esercizio della galleria – esclusa la strumentazione di controllo ferroviaria. Il CDF ha inoltre osservato l'approccio metodologico utilizzato per effettuare un'analisi dei rischi della galleria di base del San Gottardo (GBG) e della galleria di base del Ceneri (GBC), come pure la conseguente definizione e attuazione di un elenco di misure. I costi per la messa a disposizione della strumentazione di controllo ferroviaria della GBG ammontano a circa 50 milioni di franchi.

Identificazione e riduzione al minimo dei rischi mirate ma tardive

Il 1° giugno 2016 l'impresa costruttrice AlpTransit San Gottardo SA (ATG) ha consegnato la GBG all'esercente, le FFS. Dal punto di vista della sicurezza informatica, a quel momento non erano ancora state attuate tutte le misure necessarie. Esse devono ancora essere completate in base alle direttive sulla sicurezza delle TIC delle FFS. Delle analisi accurate effettuate dalle FFS mostrano che le lacune ancora esistenti al momento della messa in esercizio non presentavano rischi di livello «ROSSO», ossia intollerabili a breve e a medio termine. Inoltre, dal punto di vista della sicurezza delle TIC i rischi sono limitati al settore della disponibilità del tunnel. Nell'analisi dei rischi non sono stati rilevati pericoli dal punto di vista della sicurezza dell'esercizio, come ad esempio rischi d'incidente con danni alle persone.

Durante la fase di costruzione le FFS hanno constatato che in ambito di sicurezza delle TIC non esisteva un concetto di sicurezza generale. Ne hanno quindi allestito uno parziale di propria iniziativa per la GBG e la GBC. Su tale base e coadiuvate dalla ATG, le FFS hanno esaminato se la costituzione dell'infrastruttura allora prevista dal contratto poteva soddisfare i requisiti in materia di sicurezza. Le lacune constatate sono poi state ponderate dalle FFS in base ai loro rischi. Non sono stati rilevati rischi di livello «ROSSO». ATG e le FFS hanno allestito un piano con 42 misure di miglioramento per eliminare le lacune. Ne è scaturita una richiesta di modifica del progetto «ICT-Security GBT» del 20 maggio 2014 in cui è contemplata l'attuazione delle misure. Da una verifica sullo stato di applicazione delle misure effettuata dalle FFS prima dell'apertura della GBG è emerso che ne erano state attuate soltanto 12 e che, delle rimanenti 30, 4 erano state rinviate. Nel quadro della consegna della galleria al 1° giugno 2016, secondo ATG sono state attuate altre misure. Al momento dell'allestimento del rapporto l'efficacia di queste misure non era ancora stata verificata.

L'Ufficio federale dei trasporti deve essere rafforzato nella sua funzione di autorità di vigilanza

Il CDF constata che durante il progetto i rischi in materia di sicurezza delle TIC sono stati trattati sistematicamente solo tardivamente. Esso riconosce che l'analisi dei rischi è stata effettuata e documentata metodicamente e in modo adeguato, ma constata che ATG valuta il progresso delle misure di miglioramento diversamente dalle FFS e che le due aziende impiegano basi di valutazione diverse. Dal punto di vista del CDF ciò rischia di provocare costi supplementari e ritardi. Esso raccomanda dunque all'Ufficio federale dei trasporti (UFT) di far sorvegliare l'attuazione delle raccomandazioni ancora in sospeso. Inoltre raccomanda all'UFT di esigere, sia per la GBC sia per altri

grandi progetti di costruzione ferroviaria con imprese costruttrici diverse dagli esercenti, che presso queste ultime sia designato un organo responsabile della sicurezza delle TIC in tutte le fasi del progetto che assuma anche il ruolo di interlocutore per l'organo con la stessa funzione presso l'esercente. Questa funzione dovrebbe essere imposta anche nell'organizzazione di progetti in cui la stessa impresa funge sia da costruttrice che da esercente. Per analogia, essa dovrebbe poi fare da tramite tra l'organizzazione del progetto e dell'esercizio.

Testo originale in tedesco

Audit of the integration of the Gotthard Base Tunnel Information Technology into Swiss Federal Railways
Federal Office of Transport

Key facts

The Swiss Federal Audit Office (SFAO) examined the effectiveness of the procedure for guaranteeing an appropriate level of IT security in tunnel automation – excluding rail control technology. The SFAO also looked at the methodological approach for performing risk analysis of the Gotthard Base Tunnel (GBT) and the Ceneri Base Tunnel (CBT) and the consistent development of a set of measures and its implementation. The costs of supplying the tunnel control technology amount to approximately CHF 50 million.

Risks were identified and minimised effectively, but too late

On 1 June 2016, the constructor AlpTransit Gotthard (ATG) handed over the GTB to the operator Swiss Federal Railways (SBB). From an IT security perspective, not all of the necessary measures had been implemented by then. These have still to be completed in accordance with the SBB's ICT security requirements. The SBB's carefully executed analyses show that no risks classified as "RED" (i.e. unacceptable in the short or medium term) were to be recorded at the time of the launch of operations based on the weaknesses still present. In terms of ICT security, the risks are also limited to the area of tunnel availability. No relevant threats with regard to operational security, such as risks of accidents with personal injury, were found in the analysis of ICT security risks.

The SBB found during the construction phase that there was no overarching security concept for ICT security. As a result, it drew up the missing security concept "Subconcept (SC) for overarching ICT security GBT/CBT" on its own initiative. Based on that, and with the ATG's support, the SBB examined whether the security requirements would be met with the implementation of the infrastructure development provided for contractually at that time. The SBB then assigned a weighting to the weaknesses detected in the process based on their risks. No "RED" risks were recorded. The ATG and the SBB drew up a plan with 42 improvement measures to eliminate these weaknesses. This resulted in the project amendment request "ICT security GBT" of 20 May 2014, which covered the implementation of the measures. Prior to the opening of the GBT, the SBB verified the status of implementation of the measures and stated that only 12 had been implemented and four of the remaining 30 had been postponed. According to the ATG, further measures were implemented as part of the infrastructure handover on 1 June 2016. At the time of reporting, the effectiveness of these measures had not yet been checked.

Federal Office of Transport to be strengthened as supervisory authority

The SFAO found that the ICT security risks had not been handled systematically until late in the project. It recognises that risk analysis is performed and documented methodically and properly, but has observed that the ATG assesses the progress of the improvement measures differently to the SBB and that a different assessment basis is applied by the SBB and the ATG. From the SFAO's viewpoint, this results in a risk of additional costs and is also a cause of delays. The SFAO therefore recommends that the Federal Office of Transport (FOT) have the implementation of the still outstanding recommendations monitored. It also recommends that the FOT request a role with the constructor both for the CBT and for other major rail construction projects that have a different constructor and operator.

This role has cross-divisional responsibility for ICT security for all phases of the project and serves as an interface with a similar role with the operator. This type of role should also be requested in a project organisation for projects where the constructor and operator are the same company. It should then correspondingly form the interface between the project and the operational organisation.

Original text in German

Generelle Stellungnahme des Bundesamtes für Verkehr zur Prüfung:

Die EFK hat die Wirksamkeit des Vorgehens zur Gewährleistung eines angemessenen IT-Sicherheitsniveaus der Tunnel Betriebsautomation untersucht. Das BAV begrüsst diese Prüfung, da der Aspekt «ICT-Security» zunehmend an Bedeutung gewinnt und dies nicht nur bei den sehr langen Basistunnel, sondern bei der gesamten Eisenbahnanlage inklusive der Bahntechnik (Sicherungs-anlagen, Zugbeeinflussungssysteme und Bahnleittechnik).

Generelle Stellungnahme der SBB AG zur Prüfung:

Die Feststellungen der "Prüfung der Integration der Informatik Gotthard-Basistunnel in die SBB" durch die EFK sind aus Sicht SBB fachlich korrekt. Die abgegebenen Empfehlungen zeigen, dass die SBB bezüglich ICT-Security im GBT zeitnah und richtig gehandelt hat. Sie legt Wert auf die konsequente Umsetzung der noch offenen ICT-Security Massnahmen GBT/CBT. Die SBB begrüsst die an der Schlussbesprechung ausgesprochene Absicht des BAV, worin die noch anstehenden Fertigstellungsarbeiten der ICT-Security im GBT aus dem NEAT Kredit finanziert werden.

Die Empfehlungen der EFK zeigen ebenfalls, dass die SBB in Projekten (in denen sie als Auftraggeberin auftritt) mit den bereits eingeleiteten Massnahmen zur frühzeitigen Einbindung der Cyber Security bei Industrieanwendungen auf Kurs sind.

Generelle Stellungnahme der ATG zur Prüfung:

1. Die Empfehlungen der EFK werden durch die ATG als sinnvoll erachtet und vorbehaltlos unterstützt. Insbesondere wird (Empfehlung 2) die noch grössere Gewichtung der IT-Sicherheit der Tunnelleittechnik durch die explizite Definition und Einführung einer entsprechenden Rolle bei ATG umgehend in Angriff genommen.

2. Wir unterstützen die Auffassung, dass eine frühzeitige Abstimmung der Themen zur ICT-Security zwischen Ersteller und Betreiber von zentraler Bedeutung ist. Die ATG war deshalb bereits im Zeitraum 2009 bis 2010 bestrebt, im Rahmen der Ausführungsprojektierungsphase des GBT Projekts unter anderem die Konzepte bzw. Rahmenbedingungen im Bereich ICT-Security zusammen mit dem zukünftigen Betreiber SBB festzulegen. Die SBB war in diesem Zeitraum jedoch noch nicht in der Lage, die erforderlichen Anforderungen zu definieren. Aufgrund dieses Sachverhalts hatte die ATG die im Werkvertrag Bahntechnik als Rückfallebene vorgesehene Option „IT-Security“ ausgelöst.

Die von der SBB ab 2012 gestarteten Aktivitäten konnten infolge des fortgeschrittenen Projektstandes von ATG nur noch teilweise berücksichtigt werden. Zudem kollidierten diese mit werkvertraglichen Rahmenbedingungen sowie dem zwischen BAV, SBB und ATG am 13.06.2012 vereinbarten „Design Freeze“. Mit dem Design Freeze sollen Änderungen zu einem späten Zeitpunkt und die daraus resultieren Risiken, minimiert werden, damit die fristgerechte Fertigstellung des Werkes sichergestellt werden kann. Diese aus Sicht ATG ebenfalls relevanten Aspekte wurden im vorliegenden Bericht, aufgrund der durch die Prüfinstanz gewählten zeitlichen Abgrenzung des Prüfumfangs ab 2012 nicht berücksichtigt.

Inhaltsverzeichnis

1 Auftrag und Vorgehen

1.1 Ausgangslage

Am 1. Juni 2016 übergab die Erstellerin AlpTransit Gotthard AG (ATG) den Gotthard-Basistunnel (GBT) an die Betreiberin SBB. In Sicherheitsbelangen hat die SBB das primäre Ziel, die Gefährdung von Personen sowie unvorhersehbare Ausfälle des Tunnelbetriebes zu vermeiden. Um dieses Ziel zu erreichen, sollte die Leit- und Automatisierungstechnik des Tunnels entsprechend den auf der Norm ISO/IEC 27002:2005 beruhenden ICT-Sicherheitsvorgaben der SBB realisiert werden. Diesbezüglich führten die SBB und die ATG bereits 2012 bzw. 2013 eine Risikoanalyse durch und erstellten einen Katalog von Massnahmen zur Minimierung der erkannten Risiken. Mit Ende der Testphase per 31. Mai 2016 wurde der Betrieb der Leittechnik und der damit verbundenen Informations- und Kommunikationstechnik an die SBB übergeben. Die Kosten für den Einbau der Tunnel-Leittechnik im GBT beliefen sich auf circa 50 Millionen Franken.

1.2 Prüfungsziel und -fragen

Ziel dieser Prüfung war die Beurteilung der Wirksamkeit des Vorgehens zur Gewährleistung eines angemessenen Sicherheitsniveaus der Tunnel Betriebsautomation. Dazu sollte das methodische Vorgehen zur Erarbeitung der Risikoanalyse untersucht werden. Darauf aufbauend war die Herleitung des Massnahmenkataloges zu untersuchen. Ebenso sollten ausgewählte Prüfungssachgebiete, namentlich die Fernwartung, die Netzwerksegmentierung, die Notstromversorgung sowie die physische Sicherheit des Tunnel Control Centers in Erstfeld, vertieft bearbeitet werden.

Abgrenzung: Die gesamte Betriebsleittechnik war nicht Gegenstand dieser Prüfung.

1.3 Prüfungsumfang und -grundsätze

Die Prüfungsarbeiten fanden vom 17. Mai bis 10. Juni 2016 am Standort der Betreiberin (SBB) sowie in den Lokalitäten der Erstellerin ATG in Luzern statt. Sie basierten auf Interviews mit Schlüsselpersonen, ergänzt durch eine prüferische Durchsicht ausgewählter Projektdokumente. Ebenso nahm die EFK eine Besichtigung des Tunnel Control Centers in Erstfeld vor. Die durchgeführten Prüfungshandlungen wurden aufgrund der durch die EFK vorgenommenen Risikoanalyse zusammen mit dem darauf basierenden Prüfprogramm festgelegt. Die Prüfung wurde durch Rolf Schaffner (Leitung), Cornelia Simmen und Frank Ihle ausgeführt.

1.4 Unterlagen und Auskunftserteilung

Im Rahmen der Prüfungsarbeiten wurden die für die jeweiligen Zuständigkeitsbereiche verantwortlichen Personen der Aufsichtsbehörde (BAV), der Betreiberin (SBB) sowie der Bauherrin (ATG) beigezogen. Die erfragten Unterlagen wurden vorgelegt beziehungsweise in Form von elektronischen Dateien an die EFK abgegeben.

Die notwendigen Auskünfte wurden der EFK von allen Beteiligten in offener und konstruktiver Weise erteilt. Die EFK hatte Zugriff auf sämtliche relevanten Projekt- und Betriebsunterlagen.

2 Die wesentlichen Arbeiten aus Sicht der IT-Sicherheit

2.1 Die SBB erfasste die Infrastruktur und analysierte die ICT-Security-Risiken

Am 8. November 2006 wurde die SBB durch den Bundesrat zur Betreiberin der NEAT-Gotthard-Strecke bestimmt. Im Jahr 2012 führte die Firma [redacted] im Auftrag der SBB eine Erfassung der Architektur der Tunnelleittechnik sowie der Daten- und Kommunikationsnetze und der dafür vorgesehenen Sicherheitsmassnahmen durch und unterzog diese aus Sicht der Informationssicherheit einer ICT-Security-Risikoanalyse.

Im Fokus dieser ICT-Security-Risikoanalyse standen alle genutzten Rechnerkomponenten sowie die zugehörige Kommunikationstechnik (ICT), das heisst:

- die gesamte ICT-gestützte zentrale und dezentrale Prozess-, Leit-, Automatisierungs- und Überwachungstechnik;
- die für ihren Betrieb genutzten ICT-Systeme, beispielsweise Programmier- und Parametriergeräte;
- digitale Steuerungs- und Automatisierungskomponenten wie Leit- und Feldgeräte, Controller inklusive digitaler Sensor- und Aktorelemente und digitale Schutz- und Safetysysteme;
- die zur gewerksinternen Kommunikation eingesetzte Netzwerk-, Feldbus-, Telemetrie-, Fernwirk- und Fernsteuertechnik.

Diese Analyse stützte sich im Wesentlichen auf folgende Quellen:

- spezifisches Dokumentationsmaterial aus dem Projekt, das von der SBB zur Verfügung gestellt wurde;
- Informationen aus Befragungen der SBB-Projektingenieure anhand eines strukturierten Fragebogens zu einzelnen hierfür relevanten Leistungspaketen;
- Informationen, welche anlässlich eines Workshops mit ATG und Transtec Gotthard AG (TTG) am 28. November 2012 erhoben wurden.

2.2 Die erste Sicherheitsanalyse wies auf erhebliche Sicherheitsrisiken hin

Im „Zwischenbericht ICT-Security-Analyse für Datennetze/Rechnersysteme des Gotthard-Basistunnels“ vom 5. Februar 2013 zeigte die [redacted] auf, dass zum Zeitpunkt der Durchführung der Analyse noch nicht alle erforderlichen Informationen vorlagen. Dieser Sachverhalt wurde dadurch begründet, dass die SBB zwar die zukünftige Betreiberin sei, nicht aber die Bauherrin und ihr somit der direkte Zugang zu den einzelnen Lieferanten der ATG verwehrt gewesen wäre.

[redacted] zeigte jedoch auch auf, dass aufgrund der vorhandenen Informationen bereits erhebliche Sicherheitsrisiken identifiziert worden waren, welche grundlegend auf eine fehlende übergreifende Sicherheitskonzeption zurückzuführen waren.

2.3 Die SBB verfasste die fehlende Sicherheitskonzeption

Im Lichte dieser Feststellungen erliess die SBB per 31. Mai 2013 das „Teilkonzept übergeordnete ICT-Security GBT/CBT“. Es handelt sich dabei um ein Konzept für die übergreifende ICT-Security basierend auf ISO/IEC 27002 für das Projektvorhaben „NEAT Projekt Gotthard/Ceneri“. Die EFK hat dieses Konzept hinsichtlich seines methodologischen Aufbaus untersucht. Die entsprechenden Ergebnisse sind im Abschnitt 3 dieses Berichts dargestellt.

In der Folge prüfte die ATG auf der Basis dieses Konzepts vertieft, ob die Anforderungen mit der damals vertraglich vorgesehenen bzw. geplanten Umsetzung des Infrastrukturaufbaus erfüllt waren. Die festgestellten Abweichungen wurden als Ergebnis einer Gap-Analyse dokumentiert.

2.4 Die identifizierten Sicherheitslücken wurden nach Risiken gewichtet und ein Massnahmenplan vereinbart

Die SBB bewertete in Zusammenarbeit mit dem Projektpartner [redacted] die durch die ATG identifizierten Abweichungen gemäss den Vorgaben des „Security Handbuchs der SBB“ aus ICT-Risikosicht. Dabei wurden nur jene Abweichungen weiter betrachtet, welche nicht akzeptable ICT-Risiken nach sich zogen. Die Ergebnisse dieser Bewertung wurden im Dokument „ICT-Risikoanalyse GBT“ vom 29. November 2013 dargestellt. Zusammen mit der „ICT-Risikoanalyse GBT“ wurde der „Massnahmenkatalog GBT/CBT“ vom 29. November 2013 verfasst. In diesem Katalog sind mit Bezug auf GBT 42 Verbesserungsmassnahmen definiert.

Die ATG und die SBB definierten daraufhin Ende 2013 gemeinsam eine Projektänderung (Projektänderungsantrag „ICT-Security GBT“ vom 20. Mai 2014), um eine möglichst weitgehende Reduktion der ICT-Risiken noch vor der Übergabe des Betriebes an die SBB zu erreichen.

2.5 Die SBB überprüft den Umsetzungsstand der Verbesserungsmassnahmen

Die SBB erhob im Frühjahr 2016 über die in den Fach- und Arbeitsgruppen involvierten Life-Cycle-Manager den Umsetzungsstand der 42 Verbesserungsmassnahmen. Mit Schreiben vom 20. Mai 2016 kommunizierte die SBB ihre Sicht wie folgt an ATG:

- 12 Verbesserungsmassnahmen sind umgesetzt;
- 7 Verbesserungsmassnahmen sind teilweise umgesetzt;
- 19 Verbesserungsmassnahmen sind nicht umgesetzt;
- 4 Verbesserungsmassnahmen wurden hinsichtlich zeitlicher Umsetzung zurückgestellt.

Bezüglich dieser Beurteilung des Umsetzungsstandes der 42 vereinbarten Verbesserungsmassnahmen ist festzuhalten, dass der SBB für ihre Überprüfung nicht alle aktuellen Dokumentationen vorlagen. Diese waren gemäss der Werkverträge zwischen ATG und ihren Lieferantenfirmen erst nach dem 31. Mai 2016 zur Auslieferung an ATG vorgesehen. Somit waren sie zum Zeitpunkt der Fortschrittskontrolle durch die SBB nicht greifbar.

2.6 Keine Risiken der Einstufung „Rot“ bei der Betriebsaufnahme

Zur risikoorientierten Einstufung der identifizierten Schwachstellen wurde eine Gewichtung potenzieller Schadensereignisse nach deren Eintretenswahrscheinlichkeit und Schadensausmass vorgenommen. Im Kapitel 3.2 beurteilt die EFK die Methodik der Risikoanalyse. Ebenso sind in jenem Kapitel die angewandten Risiko-Einstufungskriterien dargestellt.

Die detailliert dokumentierten Analysearbeiten der SBB zeigen auf, dass zum Zeitpunkt der Aufnahme des Probebetriebs des GBT am 1. Juni 2016 aufgrund der noch vorhandenen Schwachstellen keine Risiken der Einstufung „ROT“ – d. h. keine kurz- und langfristig untragbaren Risiken – zu verzeichnen sind.

2.7 Die SBB beantragte das interne Projekt „ICT-Security GBT nach 2016“

Die SBB stellte dar, dass zur Erreichung einer für die SBB akzeptablen Risikosituation für den Betrieb GBT die Umsetzung aller 42 Massnahmen notwendig sei. Zur Erreichung dieser akzeptablen Risikosituation wurde seitens der SBB intern der Antrag des Projekts „ICT-Security GBT nach 2016“ gestellt. Im Rahmen dieses Projektes soll – in Abgrenzung zu den Aktivitäten der ATG – die Umsetzung der noch offenen Verbesserungsmassnahmen durch die SBB erfolgen. Die Zuständigkeiten für die Aktivitäten zur abschliessenden Umsetzung der Verbesserungsmassnahmen und insbesondre die Frage der Kostenübernahme (im Rahmen eines einstelligen Millionenbetrages) waren zwischen ATG und der SBB zum Zeitpunkt der Prüfungsdurchführung durch die EFK noch nicht geklärt. Siehe hierzu die Anmerkungen der EFK im Kapitel 3.4.

3 Beurteilung der Wirksamkeit des Vorgehens durch die EFK

Wie in den folgenden Kapiteln 3.1 bis 3.3 dargestellt, ist das Vorgehen seit dem Erlass des „Teilkonzepts übergeordnete ICT-Security GBT/CBT“ per 31. Mai 2013 durch die SBB als systematisch und fundiert zu bezeichnen. Bezüglich der Umsetzung offener Punkte und mit Blick auf zukünftige Bahnbauprojekte (siehe Kapitel 3.5) sollte das BAV als Aufsichtsbehörde entsprechende Instruktionen erlassen.

3.1 Die SBB erstellte einen klaren Katalog der IT-Sicherheitsanforderungen

In den vorangehenden Kapiteln 2.1 bis 2.4 ist dargestellt, auf welchem Weg der Status der IT-Sicherheit ermittelt wurde. Für die Untersuchung des methodischen Vorgehens ist das durch die SBB erstellte Dokument „Teilkonzept übergeordnete ICT-Security GBT/CBT“ von besonderer Relevanz. Mit diesem Teilkonzept wurde die ICT-Security der Netze und Rechnersysteme im Projekt GBT/CBT verbindlich geregelt. Es diente in der damals relevanten Fassung (31. Mai 2013) als Anforderungsdokument zur Darstellung der technischen Voraussetzungen, welche durch die ATG umzusetzen waren.

Das Teilkonzept basiert auf dem internationalen Standard ISO/IEC 27001:2005 respektive ISO/IEC 27002:2005 „Code of practice for information security management“. Es gilt über alle Leistungspakete der Bahntechnik und Lose der Rohbauausrüstung inklusive der Nahtstellen an die bestehenden SBB-Netze und Rechnersysteme. Die Vorgaben dieses Teilkonzepts gelten in der Erstellungsphase, sobald die Anlagen/Netzwerke der SBB mit denjenigen des Erstellers verbunden werden.

Die EFK beurteilt den für dieses Teilkonzept herangezogenen Standard als geeignet, um einerseits eine methodische Erhebung durchzuführen und andererseits die wichtigen Risikobereiche der ICT-Security abzudecken.

3.2 Die Methodik der Risikoanalyse ist transparent

Basierend auf dem „Teilkonzept übergeordnete ICT-Security GBT/CBT“ untersuchte die ATG, ob diese Anforderungen mit der vertraglich vorgesehenen bzw. geplanten Umsetzung erfüllt waren. Die ATG identifizierte die Abweichungen und listete diese in den folgenden Dokumenten auf:

- Liste für den Bereich RBA vom 21. Juni 2013,
- Liste für den Bereich Telecom LP6x/70 vom 19. Juli 2013,
- Erweiterte Liste für den Bereich LP60 vom 18. September 2013,
- Liste für den Bereich LP5x vom 2. Oktober 2013,
- Protokoll der Besprechung „ICT-Security“ zum Bereich SA (LP8x) am 23. September 2016.

Damit lag eine umfassende Auflistung der identifizierten Schwachstellen der ICT-Security vor.

Das Security Handbuch der SBB beschreibt im Detail die Methodik der Risikoanalyse. Im Dokument „ICT-Risikoanalyse GBT“ vom 29. November 2013 ist die risikoorientierte Beurteilung dieser Schwachstellen dargestellt. Es erfolgte eine Einstufung der einzelnen Schwachstellen hinsichtlich ihrer möglichen Schadensauswirkung sowie bezüglich ihrer Eintretenswahrscheinlichkeit.

Basierend auf den Einstufungskriterien, welche im Anhang 1 dargestellt sind, wurden die identifizierten Schwachstellen hinsichtlich ihrer Risiken beurteilt.

Die durch die EFK eingesehenen Dokumente hinterlassen den Eindruck einer fundierten und konsistent zusammenhängenden Arbeit. Das Vorgehen ist auch für einen aussenstehenden Dritten nachvollziehbar.

3.3 Der Massnahmenkatalog GBT/CBT ist nachvollziehbar und adäquat

Im „Massnahmenkatalog GBT/CBT“ vom 29. November 2013 wurden 42 für GBT relevante Verbesserungsmassnahmen dokumentiert, mit welchen die identifizierten ICT-Security-Schwachstellen behoben werden sollten.

Die EFK untersuchte, ob adäquate Verbesserungsmassnahmen definiert worden waren und ob damit die vorhandenen Schwachstellen behoben werden konnten respektive werden können. Die Bereiche „Physische Sicherheit“ und „Redundanz von Systemen“ wurden ausserhalb des Massnahmenkataloges in zusätzlichen Dokumenten behandelt.

Es wurden generelle, für alle Systeme geltende Anforderungen definiert. Ebenso wurden für die verschiedenen Gewerke spezifische Sicherheitsmassnahmen formuliert. Die Herleitung der Massnahmen zu den identifizierten Risiken bzw. Schwachstellen wurde in nachvollziehbarer Weise dokumentiert und die Massnahmen erscheinen adäquat.

3.4 ATG und die SBB beurteilen die Umsetzung der Massnahmen unterschiedlich

Wie im Kapitel 2.6 dargestellt, beurteilte die SBB den Umsetzungsstand der gemeinsam mit ATG definierten Verbesserungsmassnahmen und nahm mit Brief vom 20. Mai 2016 an die ATG Stellung dazu.

Aufgrund von Abklärungen mit der SBB und ATG stellte die EFK fest, dass für einige Verbesserungsmassnahmen bei beiden unterschiedliche Beurteilungen zum Umsetzungsstand vorlagen. Stellvertretend dafür steht die Verbesserungsmassnahme mit Referenz G-8 „Sicherstellung der mittelfristigen Verfügbarkeit des Security-Supports“, welche sich auf das Risiko „Fehlende Patch- und Update-Möglichkeit“ bezieht.

Die ATG beurteilte diese Massnahme als umgesetzt und begründet dies zum einen mit der lieferantenseitigen Gewährleistungspflicht und zum anderen damit, dass die SBB dies mit Wartungs- und Supportverträgen sicherzustellen hätte. Zudem wäre dieser Umstand bereits bei der Angebotsabgabe durch den Lieferanten über die Lebenszykluskosten ausgewiesen worden. Demgegenüber argumentierte die SBB, dass durch die ATG keine einheitlichen Vorgaben für alle Gewerke erstellt worden wären und dass auch keine entsprechenden Vollzugsmeldungen der seitens ATG zugesicherten Massnahmen vorgelegen hätten.

Seitens der EFK wurden weitere ähnlich gelagerte Fälle unterschiedlicher Umsetzungsbeurteilungen zwischen ATG und der SBB untersucht. Da einige Lieferobjekte nicht so bereitgestellt werden, wie von der SBB erwartet, besteht die Gefahr zusätzlicher Kosten und Verzögerungen für die Herstellung des durch die Betreiberin SBB vorausgesetzten Zustandes.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt dem BAV in seiner Rolle als Aufsichtsbehörde, im Rahmen der Fertigstellung des GBT den Umsetzungsfortschritt der Verbesserungsmassnahmen überprüfen zu lassen. Es hat sicherzustellen, dass die Arbeiten fristgerecht abgeschlossen werden.

Stellungnahme des Bundesamtes für Verkehr:

Das BAV unterstützt diese Empfehlung. Das BAV wird beim GBT den Umsetzungsfortschritt der erkannten Verbesserungsmassnahmen im Rahmen der ordentlichen Berichterstattung und zusätzlich im Rahmen der regelmässigen Sitzungen des Gremiums «Projektkoordination» überwachen.

3.5 Die ICT-Security wurde erst zu einem späten Zeitpunkt überprüft

Die Risiken bezüglich ICT-Security wurden erst ab 2012 systematisch analysiert. Die technologische Entwicklung im Bereich der Vernetzung industrieller Steuerungskomponenten verlief generell in den vorangehenden Jahren sehr schnell, sodass sich vielfach das entsprechende Sicherheitsbewusstsein nicht rechtzeitig bildete.

Auf dem heutigen Stand der technologischen Entwicklung sollte in den Bahnbauvorhaben die IT Sicherheit von der Planung bis zur Fertigstellung umfassend und mit angemessener Priorität berücksichtigt werden. Auf diese Weise kann sichergestellt werden, dass die IT-sicherheitsrelevanten Anforderungen bereits in frühen Phasen, wie zum Beispiel in den Ausschreibungen für Unterlieferanten, ihren Niederschlag finden. Ebenso sollten die sicherheitsrelevanten Anforderungen sowohl für die Erstellung als auch für den dauernden Betrieb (Wartung) der zu realisierenden Anlagen in umfassender Weise berücksichtigt werden.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt dem BAV, für zukünftige Bahnbauprojekte mit unterschiedlichem Ersteller und Betreiber - insbesondere für den in Umsetzung befindlichen CBT - eine Rolle beim Ersteller einzufordern, welche eine umfassende Konzeption und Umsetzung der ICT-Security über alle Phasen des Projektes übergreifend zu verantworten hat, und welche als Schnittstelle zu einer gleichartig gelagerten Rolle beim Betreiber dient.

Eine solche Rolle sollte auch bei Vorhaben, bei denen der Ersteller und der Betreiber die gleiche Gesellschaft sind, in einer Projektorganisation eingefordert werden. Sinngemäss sollte sie dann die Schnittstelle zwischen Projektorganisation und der Betriebsorganisation bilden.

Stellungnahme des Bundesamtes für Verkehr:

Das BAV unterstützt diese Empfehlung. Das BAV wird beim CBT eine umfassende Konzeption und Umsetzung der ICT-Security sowohl bei der ATG wie auch der SBB einfordern. Zudem wird das BAV das Thema «ICT-Security» bei der gesamten Eisenbahnanlage inklusive der Bahntechnik (Sicherungsanlagen, Zugbeeinflussungssysteme, Bahnleittechnik und elektrische Anlagen) betrachten. Dies betrifft sowohl neue wie auch bestehende Anlagen. Bei Bedarf wird das BAV – im Zuge einer ordentlichen Revision der hoheitlichen Vorschriften – ergänzende Vorgaben zu «ICT-Security» oder Verweise auf entsprechende bestehende Normen ins Regelwerk einfliessen lassen.

4 Ausgewählte Prüfungssachgebiete

4.1 Für die Fernwartung bestehen angemessene Sicherheitsvorkehrungen

Die Fernwartungszugriffe für Arbeiten am GBT erfolgen ausschliesslich über die Infrastruktur und entsprechend den Weisungen der SBB. Die Telecom SBB bietet eine zentrale Lösung bei der SBB im Bereich Desktop-Interaktion (Fernzugriff).

Die Sicherheitsvorkehrungen sowie die Prozesse zur Registrierung und zur Austragung von Benutzern sind im Dokument „Service Description / Service Release SR01“ Version 1.4 vom 18.12.2014 detailliert beschrieben.

Aufgrund der prüferischen Durchsicht dieses Dokuments beurteilt die EFK die beschriebenen Vorkehrungen als angemessen.

Die SBB verfügt über eine laufend aktualisierte Registratur der vergebenen Fernwartungs-Zugriffsberechtigungen. Diese Liste wurde der EFK per 9. Juni 2016 zugestellt. Aufgrund der Durchsicht durch die EFK bestehen keine Anhaltspunkte, dass diese Liste nicht vollständig ist.

4.2 Die Netzwerk-Segmentierung wird aufgeschoben

Die Segmentierung der Netzwerke ist als Massnahme Nr. 33 / LP61-6 in der Planung festgehalten. Diese Aktivität wurde aufgeschoben, da die Projektbeteiligten die hierfür notwendigen Umstellungsarbeiten als zusätzliche Risiken hinsichtlich einer zeitgerechten Inbetriebnahme einschätzten.

Die EFK hält hierzu fest, dass auch die Netzwerk-Segmentierung ein Thema ist, welches bereits in einer deutlich früheren Projektphase hätte berücksichtigt werden sollen. Auch diese Erkenntnis unterstützt die Empfehlung Nr. 2.

4.3 Die Notstromversorgung wurde implementiert und getestet

Die EFK nahm Stichproben bei den folgenden Dokumenten vor:

- Stromversorgung (inkl. Kabel 16,7 Hz) LP40 Netzberechnung 16/6 KV vom 26. Mai 2015
- Stromversorgung (inkl. Kabel 16,7 Hz) LP40 Stromversorgung / Realisierungspflichtenheft vom 30. November 2011
- Stromversorgung 50 Hz LP40 Prüfbericht zu Prüfprotokoll FAT Teil II NoB Anlage 1’000 KVA und SGK vom 19. April 2014
- Stromversorgung 50 Hz LP40 Prüfbericht zu Prüfprotokoll FAT Teil III NoB Anlage 1’600 KVA und SGK vom 2. Oktober 2014.

In diesen Dokumenten ist die Berechnung der Stromversorgungsanforderungen in den verschiedenen Spannungs- und Frequenzbändern angegeben. Die EFK erlangt hieraus keine Hinweise darauf, dass die Angaben für die benötigte Stromversorgung nicht in notwendiger Detaillierung erhoben worden wären.

Darin sind auch die Prüfprotokolle mit den entsprechenden Ergebnissen enthalten. Diese Prüfprotokolle weisen teilweise auf Schwachstellen hin, welche im Rahmen der Prüfungsdurchführungen respektive der Tests identifiziert wurden. Die SBB hat der EFK dargestellt, dass die Ergebnisse dieser Tests sowie die gegebenenfalls notwendige Umsetzung von Verbesserungsmassnahmen in die Aktivitätenplanungen eingeflossen sind.

Aufgrund der vorliegenden Unterlagen stellt die EFK keine Sachverhalte fest, die auf ungenügende Tests der installierten Anlagen hinweisen würden.

4.4 Die EFK stellt keine relevanten Mängel der physischen Sicherheit fest

Am 27. Mai 2016 besichtigte die EFK das Tunnel Control Center (TCC) in Erstfeld. Dabei stellte sie fest, dass die Zugänge zu den Räumlichkeiten klar beschrieben sind und dass eine funktional geeignete Raumaufteilung vorgenommen wurde.

Zum Zeitpunkt der Begehung durch die EFK war das Umgelände um das TCC Erstfeld noch frei begehbar. Die Vertreter der ATG zeigten der EFK auf, dass eine Umzäunung des Gebäudes und eines Teils des Umgeländes vorgesehen sei. Die Tore dieser Umzäunung würden nach der Erstellung in die Zutrittskontrollregelung miteinbezogen.

Die ATG-Vertreter informierten die EFK, dass die Zutrittsberechtigungen innerhalb des TCC in Erstfeld nach der Eröffnung des GBT am 1. Juni 2016 den damals geltenden Anforderungen entsprechend geregelt würden.

In Bezug auf die sicherheitstechnische Gebäudeausrüstung hat die EFK aufgrund ihrer Besichtigung keine offensichtlichen Mängel festgestellt.

5 Schlussbesprechung

Die Schlussbesprechung fand am 13. Juli 2016 statt. Teilgenommen haben aufseiten der SBB der Leiter PONS, verantwortlich für die Inbetriebnahme des Gotthardtunnels, der Leiter ICT Security, Risk und Compliance Management und der Head ICT Risk Management, ferner zwei Mitarbeiter der ATG und ein Berater im Auftrag der ATG, schliesslich aufseiten des BAV der Sektionschef Sicherheitstechnik sowie der Stellvertreter Grossprojekte.

Die EFK war vertreten durch den Leiter Fachbereich 4, den Mandatsleiter 3 und den Revisionsleiter.

Bezüglich der wesentlichen Feststellungen und Empfehlungen an der Schlussbesprechung bestand Übereinstimmung.

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

EIDGENÖSSISCHE FINANZKONTROLLE

Anhang 1: Skala zur Einstufung der Risiken

Für die **Schadensauswirkung** wurden folgende Stufen angewandt:

- Sehr klein: Ausfall mit lokal beschränkter Tragweite bis 1 Tag
- Klein: Ausfall mit regionaler Tragweite < 1 Tag bzw. mit lokaler Tragweite > 1 Tag
- Mittel: Ausfall mit nationaler Tragweite < 1 Tag bzw. mit regionaler Tragweite > 1 Woche
- Mittel gross: Ausfall mit nationaler Tragweite bis zu 1 Woche bzw. mit regionaler Tragweite > 1 Woche
- Gross: Ausfall nationaler Tragweite bis zu 1 Monat
- Sehr gross: Ausfall mit nationaler Tragweite > 1 Monat

Die **Eintretenswahrscheinlichkeit** beurteilt die Wahrscheinlichkeit des Schadenseintrittes *innerhalb eines Jahres*. Hierfür wurden folgende Einstufungen vorgenommen:

- Sehr klein: 0 bis 10 %
- Klein: 10 bis 30 %
- Mittel: 30 bis 50 %
- Gross: 70 bis 85 %
- Sehr gross: > 85 %

Die Ausprägung der **Risikoeinstufung ROT** bedeutet, dass das Risiko auch kurzfristig nicht akzeptierbar ist. Es muss im Rahmen der Risikosteuerung umgehend und mit allen erforderlichen Ressourcen vermieden, vermindert, übertragen bzw. abgesichert werden.

In diese Einstufung fallen Risiken bei denen

- die Eintretenswahrscheinlichkeit/Jahr als sehr gross und das Schadensausmass mindestens als klein oder
- die Eintretenswahrscheinlichkeit/Jahr als gross und das Schadensausmass mindestens als mittel gross oder
- die Eintretenswahrscheinlichkeit/Jahr als mittel und das Schadensausmass mindestens als gross oder
- die Eintretenswahrscheinlichkeit/Jahr als mittel oder klein und das Schadensausmass als sehr gross

beurteilt wurden.

(Quelle: Dokument „ICT-Risikoanalyse GBT“ vom 29. November 2013)

Anhang 2: Rechtsgrundlagen, Priorisierung der Empfehlungen

Rechtsgrundlagen

Finanzkontrollgesetz (FKG, SR 614.0)

Finanzhaushaltgesetz (FHG, SR 611.0)

Finanzhaushaltverordnung (FHV, SR 611.01)

Bundesinformatikverordnung (BinfV, SR 172.010.58)

ISO/IEC 27001:2005 bzw. ISO/IEC 27002:2005 (diese Standards spezifizieren Anforderungen für die Implementierung geeigneter IT-Sicherheitsmechanismen)

Priorisierung der Empfehlungen

Die EFK priorisiert die Empfehlungen nach den zugrunde liegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).

Anhang 3: Abkürzungen, Glossar,

Abkürzungen

ATG	AlpTransit AG (Erstellerin bzw. Bauherrin des Gotthard-Basistunnels)
BAV	Bundesamt für Verkehr
CBT	Ceneri-Basistunnel
GBT	Gotthard-Basistunnel
SBB	Schweizerische Bundesbahnen
TCC	Tunnel Control Center
TTG	Transtec Gotthard AG

Glossar

Tunnel Control Center	Für den Gotthard-Basistunnel bestehen die zwei Tunnel Control Center in Bodio (TI) und in Erstfeld (UR). Es handelt sich hier um die Lokalitäten für die Steuerung der Tunnelbetriebsautomation.
Transtec Gotthard AG	Transtec Gotthard ist eine Arbeitsgemeinschaft von den in ihren Bereichen führenden Unternehmen Alpiq, Alcatel-Lucent/Thales, Heitkamp Construction Swiss (ehemals Alpine-Bau) und Balfour Beatty Rail.
Rohbauausrüstung	Die Einbauten der Rohbauausrüstung umfassen Belüftungs-, Wasserversorgungs- und Entwässerungsanlagen, aber auch Klimaanlagen für Gebäude, Krananlagen, Türen, Doppelböden, Metallkonstruktionen sowie Elektro- und Brandschutzinstallationen.