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

Prüfung des Programms Datacom-NG

Schweizerische Bundesbahnen

EFK-19346 | inkl. Stellungnahmen | 19. Dezember 2019 | FinDel D1/2020

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45 3003 Bern Schweiz
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	1.19346.916.00415
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch twitter: @EFK_CDF_SFAO + 41 58 463 11 11
Abdruck Reproduction Riproduzione Reprint	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

Inhaltsverzeichnis

Prüfung des Programms Datacom-NG
Schweizerische Bundesbahnen

Das Wesentliche in Kürze

Mit dem nationalen Datennetz verbindet die Schweizerischen Bundesbahnen (SBB) AG sämtliche Systeme der Bahnproduktion, der Kommunikation sowie die Arbeitsplatzsysteme der Mitarbeitenden. Das seit 2005 in Betrieb stehende Netzwerk wird nun im Rahmen des Programms «Datacom-NG» abgelöst. Die Komponenten und Technologien werden durch eine leistungsfähigere Generation ersetzt. Mit dem Rückbau der veralteten Infrastruktur soll das Programm spätestens 2022 abgeschlossen sein.

Die Eidgenössische Finanzkontrolle (EFK) hat das Programm «Datacom-NG» geprüft. Die Ergebnisse zeigen, dass die Umsetzung zeitlich und inhaltlich auf Kurs ist. Rund 80 % der geplanten Strecken sind realisiert und in Betrieb. Die Migration der Dienste auf das neue Netz ist komplex. Die SBB AG begegnet dieser Herausforderung mit laufenden Prozessoptimierungen und eine hohe Automatisierung. Eine weitere Herausforderung fällt dem Bundesamt für Verkehr (BAV) mit der Optimierung der Bewilligungsverfahren zu.

Der Umfang und die Kosten wurden massiv unterschätzt

Das Programm wurde 2014 durch den Verwaltungsrat (VR) der SBB AG genehmigt und ein geplanter Rahmenkredit von 155 Millionen Franken bewilligt. Der VR hat die SBB Infrastruktur mit der Umsetzung des Programms im Bereich Telecom beauftragt. 2018 wurde das Kostendach auf 185 Millionen Franken erhöht. Zum Prüfungszeitpunkt sind rund 160 Millionen Franken aufgelaufen. Damit die weiter anfallenden Kosten bis zum Programmende gedeckt werden können, soll das Budget auf bis zu 275 Millionen Franken erhöht werden.

Diese massive Kostenentwicklung hat zwei Gründe: Einerseits wurden der Umfang der Anforderungen und Dienste im Zuge der stark voranschreitenden Digitalisierung erweitert, andererseits mussten die Werkzeuge im Bereich der Automatisierung weiterentwickelt werden, um das starke Mengenwachstum bewältigen zu können. Diese Aufwände wurden teils fälschlicherweise dem Programm zugeordnet. Eine Aufarbeitung der finanziellen Situation wurde 2018 nach einem Wechsel in der Programmführung initiiert. Um den Schwachstellen im Controlling zu begegnen, führte die neue Führung wirkungsvollere Instrumente für das Controlling und das Reporting ein.

Die EFK empfiehlt der SBB AG, in zukünftigen IKT-Vorhaben der Infrastruktur, ein stringentes Controlling der relevanten Kostentreiber umzusetzen. Ein durch den Leiter Infrastruktur in Auftrag gegebenes unabhängiges Audit soll die finanzielle und organisatorische Situation im Programm klären.

Eine einheitliche Projekt- und Risikomanagement-Methode fehlt

Seit dem Wechsel des Programmleiters wurden zahlreiche Massnahmen und Werkzeuge zur besseren Steuerung des Programms umgesetzt. Das Programmmanagement und die Organisation sind aus Sicht der EFK heute zweckmässig aufgestellt.

Die Division Infrastruktur bedient sich für die Führung von Projekten mehrheitlich der Normen des Schweizerischen Ingenieur- und Architektenverein für Bauprojekte. IKT-Projekte

können aufgrund der sich rasch wandelnden Charakteristik und Anforderungen nicht mit diesen Methoden geführt werden. Für SBB Telecom bestehen keine einheitlichen Vorgaben für das Projektmanagement. Solche sind für eine effiziente Führung und ein entsprechendes Controlling unabdingbar. Die EFK hat dazu eine Empfehlung abgegeben.

Der Risikomanagementprozess ist fester Bestandteil im Programm. Das unternehmensweite Werkzeug zur Erfassung der Risiken ist für Vorhaben dieser Art ungeeignet und wird daher bei «Datacom-NG» nicht eingesetzt. Anderweitige Vorgaben oder Instrumente zur Risikobehandlung stehen nicht zur Verfügung. Dadurch werden Risiken in unterschiedlichen Instrumenten erfasst und regelmässig in einer konsolidierten Form an die übergeordneten Stellen rapportiert. Dies erschwert die Aggregation bzw. Konsolidierung sowie die Herleitung und Nachvollziehbarkeit der Risiken auf Stufe Konzern erheblich. Die EFK empfiehlt der SBB AG, eine einheitliche Methodik zu erarbeiten.

Die Sicherheit in Teilnetzen und im Betrieb soll verbessert werden

Die konzernweiten Vorgaben zur IT-Sicherheit weisen allgemein eine hohe Qualität auf. Deren Umsetzung in Projekten wird vor der Inbetriebnahme durch eine unabhängige Stelle geprüft. Bei länger dauernden Vorhaben ist jedoch keine periodische Prüfung im Projektverlauf vorgesehen, dies auch nicht bei Abweichungen zu den genehmigten Konzepten.

Die Netzwerkarchitektur zielt auf eine hohe Verfügbarkeit ab. Gängige Mechanismen und Werkzeuge zur Absicherung der Netzwerke sind weitgehend implementiert. Wichtige Sicherheitsvorkehrungen in Teilnetzen sind zum Zeitpunkt der Prüfung nicht gemäss Pflichtenheft umgesetzt resp. aktiv.

Die Organisation des Betriebes ist auf einem hohen Niveau. Eine Datensicherung der Managementsysteme erfolgt regelmässig. Tests zur Wiederherstellung wurden jedoch nur bei der Inbetriebnahme durchgeführt und werden nicht regelmässig wiederholt. Nur regelmässige Tests der Datenwiederherstellung stellen sicher, dass im Ereignisfall auf funktionierende Prozesse zurückgegriffen werden kann.

Die SBB AG hat einen angemessenen Prozess zur Bearbeitung von Sicherheitsvorfällen. Ereignisse werden mit unterschiedlichen Werkzeugen erfasst, bearbeitet und wo nötig eskaliert. Bei Verwundbarkeiten der Infrastruktur verlässt sich die SBB AG noch auf den Lieferanten. Der Prozess sowie die Hilfsmittel zur aktiven Erkennung von Sicherheitsvorfällen und von Verwundbarkeiten existiert heute nur in Ansätzen.

Unspezifische Vorgaben zur IT-Sicherheit

Das BAV sorgt als Aufsichtsbehörde für ein hohes Sicherheitsniveau im Schienenverkehr. Es ist Bewilligungsbehörde für Neu- und Umbauten der Eisenbahninfrastruktur. Seit 2010 fordert das BAV bei jedem Plangenehmigungsverfahren ein Sicherheitsmanagementsystem, welches die IT-Sicherheit beschreibt, ohne jedoch detaillierte Vorgaben zu machen. Diese Anforderung soll gemäss BAV in den überarbeiteten Ausführungsbestimmungen zur Eisenbahnverordnung Ende 2020 klarer definiert und verankert werden.

Das dynamische Umfeld der Bahnbetreiberinnen bringt regelmässige Änderungen in der Systemlandschaft mit sich. Solche Anpassungen erfordern jeweils eine erneute und zeitnahe Zulassung durch das BAV. Das Bewilligungsverfahren verursacht heute eine verhältnismässig grosse zeitliche Verzögerung bei der Implementierung von Massnahmen. Die EFK empfiehlt dem BAV, eine Optimierung des Verfahrens hinsichtlich der Durchlaufzeiten zu prüfen.

Audit du programme Datacom-NG
Chemins de fer fédéraux

L'essentiel en bref

Le réseau national de données des Chemins de fer fédéraux (CFF) SA relie tous les systèmes de production ferroviaire, de communication ainsi que les systèmes de postes de travail des collaborateurs. En place depuis 2005, le réseau sera prochainement remplacé dans le cadre du programme « Datacom-NG ». Les composants et les technologies seront remplacés par une génération plus performante. Le programme doit s'achever avec le démantèlement de l'infrastructure obsolète, en 2022 au plus tard.

Le Contrôle fédéral des finances (CDF) a examiné le programme « Datacom-NG ». Les résultats montrent que la mise en œuvre se déroule comme prévu sur les plans du calendrier et des contenus. Près de 80 % des lignes prévues sont réalisées et en service. La migration des services sur le nouveau réseau est complexe. Les CFF SA relèvent ce défi en optimisant continuellement leurs processus et en recourant à un haut degré d'automatisation. L'Office fédéral des transports (OFT) doit quant à lui relever un autre défi avec l'optimisation des procédures d'autorisation.

Sous-estimation massive de l'ampleur et des coûts

Le conseil d'administration des CFF SA a approuvé le programme en 2014 et débloqué le crédit-cadre prévu de 155 millions de francs. Il a confié la mise en œuvre du programme, qui appartient au domaine des télécommunications, à CFF Infrastructure. En 2018, le plafond des coûts a été relevé à 185 millions de francs. Au moment de l'audit, quelque 160 millions de francs avaient été dépensés. Afin de couvrir la totalité des frais jusqu'à à la fin du programme, le budget doit être porté à 275 millions de francs.

Cette hausse considérable tient à deux facteurs: d'une part, le développement rapide du numérique a amplifié les exigences et les services, d'autre part, il a fallu développer les outils dans le domaine de l'automatisation afin de maîtriser la forte augmentation des volumes. Certaines de ces dépenses ont été attribuées à tort au programme. Un bilan de la situation financière a été lancé en 2018 suite au changement au sein de la direction du programme. Pour remédier aux faiblesses dans le domaine du controlling, la nouvelle direction a mis en place des instruments de contrôle et de compte rendu plus efficaces.

Le CDF recommande aux CFF SA d'appliquer aux futurs projets d'infrastructure TIC un contrôle rigoureux des facteurs de coûts importants. Le directeur de CFF Infrastructure a commandé un audit indépendant pour faire le point sur l'état des finances et de l'organisation du programme.

Il manque une méthode uniforme de gestion des projets et des risques

Depuis l'arrivée du nouveau responsable de programme, de nombreux outils et mesures visant à améliorer le pilotage ont été mis en œuvre. Le CDF estime aujourd'hui que la gestion et l'organisation du programme sont appropriées.

Pour la conduite de ses projets, la division Infrastructure applique souvent les normes de la Société suisse des ingénieurs et des architectes. Ces méthodes ne conviennent pas pour les

projets TIC, dont les caractéristiques et les exigences évoluent vite. CFF Telecom n'a pas de directives uniformes pour la gestion de projets, or celles-ci sont indispensables à une gestion efficace et à un contrôle approprié. Le CDF a émis une recommandation à ce sujet.

Le processus de gestion des risques fait partie intégrante du programme. L'outil de saisie des risques utilisé dans l'ensemble de l'entreprise ne convient pas pour les projets de cette nature et n'est donc pas employé pour « Datacom-NG ». Il n'existe pas d'autres directives ou instruments pour traiter les risques. Ainsi, ces derniers sont saisis dans différents outils et rapportés régulièrement à la hiérarchie sous une forme consolidée. Cette procédure complique beaucoup l'agrégation ou la consolidation des risques de même que leur traçabilité au niveau du groupe. Le CDF recommande aux CFF SA d'élaborer une méthode uniforme.

Nécessité d'améliorer la sécurité des sous-réseaux et de l'exploitation

Les directives du groupe en matière de sécurité informatique sont généralement de grande qualité. Leur mise en œuvre dans les projets est contrôlée par un organisme indépendant avant leur mise en service. Toutefois, dans le cas de projets de plus longue durée, aucun examen périodique n'est prévu, même si les concepts approuvés initialement sont modifiés en cours de route.

L'architecture des réseaux vise à offrir une grande disponibilité. Les réseaux sont protégés par des mécanismes et des outils courants largement implémentés. Des mesures de sécurité importantes prévues par le cahier des charges pour certains sous-réseaux n'étaient pas en place ou pas activées au moment de l'audit.

L'exploitation obéit à une organisation de haut niveau. Les données des systèmes de gestion sont sauvegardées à intervalles réguliers. Des tests de récupération ont eu lieu lors de la mise en service, mais ils ne sont pas renouvelés périodiquement. Or seuls des tests réguliers permettent de s'assurer que les processus fiables restent accessibles en cas d'incident.

Les CFF SA disposent d'une procédure appropriée de traitement des incidents de sécurité. Différents instruments servent à identifier, à traiter et, si nécessaire, à faire remonter les incidents. En cas de vulnérabilité de l'infrastructure, les CFF SA s'en remettent encore aux fournisseurs. Le processus et les outils de détection active des incidents de sécurité et des vulnérabilités ne sont aujourd'hui qu'au stade de la conception.

Directives non spécifiques en matière de sécurité informatique

En tant qu'autorité de surveillance, l'OFT assure un niveau de sécurité élevé dans le trafic ferroviaire. Il est aussi chargé d'approuver les nouvelles constructions ou les transformations de l'infrastructure ferroviaire. Depuis 2010, il exige un système de gestion de la sécurité pour chaque procédure d'approbation des plans, qui décrit la sécurité informatique, sans pour autant donner des directives détaillées. Selon l'OFT, cette exigence doit être définie plus clairement et inscrite dans les dispositions d'exécution révisées de l'ordonnance sur les chemins de fer fin 2020.

L'environnement très dynamique des opérateurs ferroviaires entraîne des modifications fréquentes de l'infrastructure des systèmes, lesquelles requièrent à chaque fois l'autorisation, dans les meilleurs délais, de l'OFT. La procédure d'autorisation occasionne actuellement des retards relativement importants dans la mise en œuvre des mesures. Le CDF recommande à l'OFT d'examiner une optimisation des processus quant aux délais d'exécution.

Texte original en allemand

Verifica del programma Datacom-NG
Ferrovie federali svizzere

L'essenziale in breve

La rete nazionale di dati delle Ferrovie federali svizzere (FFS) SA collega tutti i sistemi della produzione ferroviaria e della comunicazione nonché i sistemi di postazioni di lavoro dei collaboratori. La rete in uso dal 2005 verrà sostituita nel quadro del programma «Datacom-NG». Le componenti e le tecnologie verranno sostituite da una generazione più performante. Il programma si concluderà al più tardi nel 2022 con lo smantellamento dell'infrastruttura divenuta obsoleta.

Il Controllo federale delle finanze (CDF) ha esaminato il programma «Datacom-NG». I risultati mostrano che l'attuazione sta procedendo come previsto sia sul piano temporale che su quello materiale. Circa l'80 per cento delle tratte previste sono state realizzate e sono in funzione. La migrazione dei servizi sulla nuova rete è complessa. Le FFS SA affrontano questa sfida ottimizzando costantemente i processi e applicando un elevato tasso di automazione. L'Ufficio federale dei trasporti (UFT) deve affrontare l'ulteriore sfida dell'ottimizzazione della procedura di autorizzazione.

L'estensione dei requisiti e dei servizi e i costi sono stati fortemente sottovalutati

Nel 2014 il consiglio d'amministrazione delle FFS SA ha approvato il programma e ha stanziato il credito quadro previsto di 155 milioni di franchi. L'organo ha incaricato FFS Infrastruttura di attuare il programma, che riguarda il settore della telecomunicazione. Nel 2018 l'importo massimo dei costi è stato aumentato a 185 milioni di franchi. Al momento della verifica sono stati spesi circa 160 milioni di franchi. Per coprire gli ulteriori costi che si verificheranno fino alla fine del programma, il credito deve essere innalzato a 275 milioni di franchi.

Quest'impennata dei costi è dovuta a due fattori: da un lato, il progressivo sviluppo della digitalizzazione ha determinato un'estensione dei requisiti e dei servizi e, dall'altro, per far fronte al forte aumento delle quantità è stato necessario sviluppare gli strumenti nel campo dell'automazione. Queste spese sono state attribuite al programma, in parte per sbaglio. Dopo un cambiamento nella direzione del progetto, nel 2018 è stata avviata un'analisi della situazione finanziaria. La nuova direzione ha introdotto strumenti più efficaci per il controllo e il rendiconto al fine di colmare le lacune in questi ambiti.

Per i futuri progetti TIC connessi all'infrastruttura, il CDF raccomanda alle FFS SA di effettuare un controllo più rigoroso dei fattori di costo rilevanti. Una verifica indipendente commissionata dal direttore di FFS Infrastruttura mira a chiarire la situazione finanziaria e organizzativa del programma.

Manca un metodo uniforme di gestione dei progetti e dei rischi

Dall'arrivo del nuovo responsabile del programma sono stati applicati numerosi strumenti e misure per migliorare il controllo del programma. Secondo il CDF ora la gestione del programma e l'organizzazione sono adeguate.

Per la gestione dei progetti la divisione Infrastruttura si basa prevalentemente sulle norme della Società svizzera degli ingegneri e degli architetti. I progetti TIC non possono essere gestiti

con questi metodi poiché le loro caratteristiche e i loro requisiti evolvono rapidamente. Telecom FFS non dispone di prescrizioni uniformi per la gestione dei progetti, che sono però indispensabili per una gestione e un controllo efficienti. Il CDF ha formulato una raccomandazione al riguardo.

Il processo di gestione dei rischi è parte integrante del programma. Lo strumento di rilevazione dei rischi utilizzato in tutta l'azienda non è idoneo per progetti di questo tipo e quindi non viene impiegato per il programma «Datacom-NG». Non sono però disponibili altri strumenti o prescrizioni per il trattamento dei rischi, che vengono quindi rilevati con strumenti diversi e riferiti regolarmente in forma consolidata ai servizi gerarchicamente sovraordinati. Questa procedura complica notevolmente l'aggregazione, ossia il consolidamento, e la tracciabilità dei rischi a livello di gruppo. Il CDF raccomanda alle FFS SA di elaborare un metodo uniforme.

Occorre migliorare la sicurezza nelle sottoreti e nell'esercizio

Le prescrizioni vigenti a livello di gruppo relative alla sicurezza informatica sono generalmente di qualità elevata. La loro attuazione nei progetti viene esaminata da un organismo indipendente prima della messa in esercizio. Tuttavia, non è prevista alcuna verifica periodica per i progetti di lunga durata, nemmeno in caso di modifiche rispetto ai piani approvati.

L'architettura della rete mira a offrire un'elevata disponibilità. Per proteggere le reti sono stati implementati su vasta scala meccanismi e strumenti comuni, ma al momento della verifica non erano state attuate o attivate importanti misure di sicurezza previste dal capitolato d'oneri per le sottoreti.

L'organizzazione dell'esercizio è di alto livello. Il backup dei sistemi di gestione viene effettuato regolarmente. Tuttavia, i test di ripristino sono stati svolti solo al momento della messa in esercizio e non vengono ripetuti periodicamente. Soltanto testando regolarmente il ripristino dei dati si garantisce il ricorso a processi funzionanti in caso di incidenti.

Le FFS SA dispongono di una procedura adeguata per trattare gli incidenti legati alla sicurezza. Si utilizzano diversi strumenti per rilevare gli incidenti, trattarli e, se necessario, demandarli al livello gerarchico superiore. In caso di vulnerabilità dell'infrastruttura, le FFS SA si affidano ancora ai fornitori. Attualmente, il processo e gli ausili per riconoscere attivamente gli incidenti legati alla sicurezza e le vulnerabilità non sono ancora completamente sviluppati.

Prescrizioni non specifiche relative alla sicurezza informatica

In veste di autorità di vigilanza, l'UFT provvede affinché il traffico ferroviario presenti un livello di sicurezza elevato. È anche incaricato di autorizzare le nuove costruzioni e i lavori di trasformazione dell'infrastruttura ferroviaria. Dal 2010, per ogni procedura di approvazione dei piani, l'UFT richiede un sistema di gestione della sicurezza che descriva la sicurezza informatica, senza però formulare prescrizioni dettagliate. Secondo l'UFT questo requisito dovrà essere definito più chiaramente e inserito a fine 2020 nelle disposizioni d'esecuzione rielaborate dell'ordinanza sulle ferrovie.

L'ambiente dinamico in cui operano le imprese ferroviarie comporta modifiche regolari dell'ambiente del sistema, che richiedono ogni volta il rilascio tempestivo di una nuova autorizzazione da parte dell'UFT. Attualmente la procedura di autorizzazione causa un ritardo relativamente importante nell'implementazione delle misure. Il CDF raccomanda all'UFT di valutare un'ottimizzazione della procedura per quanto concerne i tempi di esecuzione.

Testo originale in tedesco

Program audit of Datacom-NG
Swiss Federal Railways

Key facts

The Swiss Federal Railways (SBB) AG use the national data network to connect all systems for railway operations and communications, as well as the employee workplace systems. The network, which has been in operation since 2005, is now being replaced as part of the Datacom-NG program. Components and technologies are due to be replaced by a more powerful generation. Program completion is scheduled for 2022 at the latest, with the dismantling of the obsolete infrastructure.

The Swiss Federal Audit Office (SFAO) has audited the Datacom-NG program. The results show that implementation is on track in terms of both timetable and content. Around 80% of the planned lines have been completed and are in operation. Migrating the services to the new network is a complex undertaking. SBB AG is meeting the challenge with ongoing process optimisation and a high degree of automation. The Federal Office of Transport (FOT) is also facing a challenge, in the form of the optimisation of approval procedures.

Scope and costs were grossly underestimated

The program was approved by SBB AG's board of directors in 2014 and a planned framework credit of CHF 155 million was authorised. The board commissioned the SBB's Infrastructure division to implement the program for the telecoms area. In 2018, the cost ceiling was raised to CHF 185 million. At the time of the audit, costs amounted to around CHF 160 million. In order to cover the remaining costs that will accrue by the end of the project, the budget should be increased to CHF 275 million.

The reasons for this huge increase in costs are twofold: First, the scope of the requirements and services was expanded in light of rapidly advancing digitalisation; second, automation tools had to be upgraded to deal with the significant growth in volume. Some of the related expenditure was erroneously allocated to the program. In 2018, following a change of program leader, the financial situation was reviewed. In order to remedy the weaknesses in controlling, the new program leader introduced more effective controlling and reporting tools.

The SFAO recommends that SBB AG should implement stringent controlling for the relevant cost drivers in the Infrastructure division's future ICT projects. An independent audit has been commissioned by the Head of Infrastructure to clarify the program's finances and organisation.

Lack of consistency in project and risk management methods

Since the change of program head, a number of measures and tools have been implemented to improve program management. In the SFAO's view, program management and organisation are now appropriately structured.

For managing most of its projects, the Infrastructure division uses the standards of the Swiss Society of Engineers and Architects. Owing to their rapidly changing nature and requirements, ICT projects cannot be managed with these methods. There are no consistent regulations on SBB Telecom project management. These are indispensable for efficient management and appropriate controlling. The SFAO has made a recommendation in this regard.

The risk management process is an integral part of the program. The company-wide tool for capturing risk is unsuitable for this kind of project and is thus not used for Datacom-NG. Other risk management rules or tools are not available. As a result, risks are captured using a variety of tools and are regularly reported up the line in consolidated form. This makes it much more difficult to aggregate and consolidate risks, to identify their origin and to understand their significance for the group as a whole. The SFAO recommends that SBB AG should draw up a consistent methodology.

Security in subnetworks and operations should be improved

The group-wide rules on IT security are generally of high quality. Their implementation in projects is reviewed by an independent body before the start of operations. For longer projects, however, no regular checks during the life of the project are planned, even in the case of deviations from the approved strategies.

The network architecture is aimed at providing high availability. Common network security mechanisms and tools are widely used. At the time of the audit, important security precautions in subnetworks were either not being implemented as per the specifications or were not active.

The operation is highly organised, with regular data backups of management systems. Yet recovery tests were only performed at the start of operations and are not repeated on a regular basis. Only regular testing of data recovery will ensure access to functioning processes in the event of an incident.

SBB AG has an appropriate process for managing security incidents. They are recorded, processed and escalated as necessary, using various tools. As regards vulnerabilities in the infrastructure, SBB AG still relies on its suppliers. Currently, there are only rudimentary processes and tools for actively detecting security incidents and vulnerabilities.

Non-specific IT security rules

As the supervisory authority, the FOT ensures a high level of security in rail transportation. It is the approval authority for new railway infrastructure and for alterations. Since 2010, the FOT has stipulated that each approval procedure must feature a security management system which describes the IT security, but has not set detailed requirements. According to the FOT, this stipulation is to be more clearly defined and anchored in the revised implementing provisions to the Railways Ordinance at the end of 2020.

The dynamic environment for rail operators means that the system landscape changes regularly. Each adjustment requires new and timely approval by the FOT. With the current approval procedure, there is a relatively long lag before measures can be implemented. The SFAO recommends that the FOT review its procedures with a view to optimising turnaround times.

Original text in German

Generelle Stellungnahme der Geprüften

Generelle Stellungnahme SBB

Das neue Datennetz der SBB AG Datacom-NG ersetzt das bestehende und vernetzt alle relevanten Dienste der Bahnproduktion und der Bürokommunikation. Die Anforderungen an Digitalisierung, Automatisierung und Wachstum sind deutlich zu spüren. Die SBB AG ist sich der wachsenden Bedeutung des Datennetzes bewusst und ist bestrebt mit dieser Infrastruktur auch zukünftige Anforderungen erfüllen zu können. Die SBB AG befindet sich in einem starken digitalen Wandel und hat viele Initiativen gestartet um die eigene Organisation, Programme und Projekte besser auf die Herausforderungen der Digitalisierung vorzubereiten. Sie begrüsst die objektive Prüfung durch die EFK und bedankt sich für die wertvollen Anregungen für das Programm und auch die gesamte Organisation, um diesen Wandel weiter vorantreiben zu können. Die Prüfung der EFK über das Programm Datacom-NG zur Erstellung eines neuen Datennetzes hat in einem konstruktiven Rahmen stattgefunden. Die Empfehlungen der EFK wurden als gute und zielführende Punkte erkannt, welche im weiteren Verlauf in das Programm Datacom-NG und in überordnete Vorgabedokumente einfliessen werden.

Generelle Stellungnahme BAV

Die im EFK-Bericht aufgeworfenen Themen standen im Fokus des Typenzulassungsprozesses des Datennetzes Datacom-NG, welcher zum Zeitpunkt der Prüfung durch die EFK noch in der Erprobungsphase war.

Der Prozess Datennetze@SA, der Bestandteil der Typenzulassung ist, berücksichtigt die aufgeworfenen Themen vollumfänglich.

Das BAV untersucht gegenwärtig mit der Branche, wie die Migration und der Betrieb von neuen Datennetzen bei den übrigen Bahnen ähnlich effizient behandelt werden kann.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Der Bahnverkehr ist ein Teil der kritischen Infrastruktur (KI) der Schweiz. Störungen im Schienenverkehr wirken sich auf nahezu alle Lebensbereiche aus. Betroffen ist insbesondere die Wirtschaft, aber auch die Bevölkerung wird durch länger anhaltende Störungen nachhaltig beeinträchtigt. Der Schienenverkehr ist stark von der Funktionsfähigkeit von technischen Infrastrukturdiensten, wie z. B. der Stromversorgung oder den Informations- und Kommunikationstechnologien (IKT), abhängig. Die SBB AG betreibt ein eigenes schweizweites Datennetz mit hohen Anforderungen an die Verfügbarkeit und Resilienz.

Der Bereich Telecom (I-AT-TC) der SBB Infrastruktur löst mit dem Programm «Datacom-NG» das seit 2005 in Betrieb stehende und inzwischen veraltete Datennetz ab. Im Mai 2014 hat der Verwaltungsrat (VR) der SBB AG hierfür einen Kredit von 155 Millionen Franken bewilligt. Die Auftragsvergabe erfolgte am 15. Januar 2016 nach einem selektiven Verfahren gemäss dem Bundesgesetz und der Verordnung über das öffentliche Beschaffungswesen (BöB/VöB). Die Erneuerung wird in mehreren Etappen durchgeführt und befindet sich mit der Migration der bahnkritischen Anwendungen seit 2019 in der Schlussphase. Nach Rückbau der veralteten Infrastruktur soll das Programm spätestens 2022 abgeschlossen sein.

Die bestehenden Systeme werden durch neue, leistungsfähigere Komponenten hinsichtlich Funktionalität, Bandbreite und Netzabdeckung ersetzt. Ziel ist die Sicherstellung der Grundversorgung der SBB AG mit Telekommunikationsleistungen bei hoher Qualität, Sicherheit und Verfügbarkeit. Zudem soll die Bereitstellung der nötigen Managementsysteme für eine effiziente Service-Provisionierung, ein effizientes Incident- und Problem-Handling sowie die Konfiguration und Verwaltung der Netzwerkressourcen aufgebaut werden.

Eine Trennung der bahnbetriebskritischen Anwendungen von den nicht für den Bahnbetrieb sensiblen Anwendungen ist in separaten Zonen sichergestellt. Die Netze sind wo nötig redundant aufgebaut.

- Das optische Übertragungsnetz ist physikalisch redundant ausgelegt (gelb / blau).
- Das Anschlussnetz für bahnbetriebskritische Anwendungen, Rail Data (rot / grün), ist ebenfalls redundant aufgebaut (zwei physisch getrennte Geräte am Service Access Point, zwei physisch getrennte Netze).
- Das Anschlussnetz für Kunden- und Bürosysteme und bahnbetriebsnahe Systeme, Business Data (schwarz).

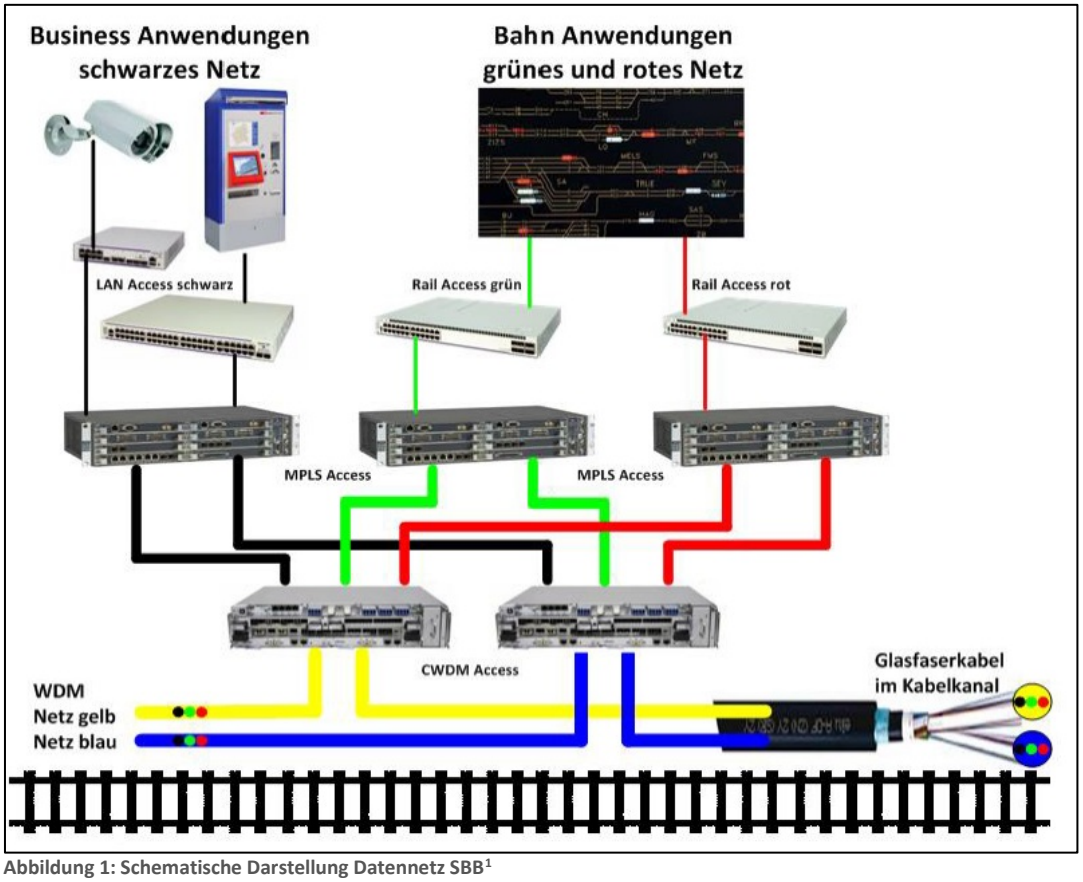

Abbildung 1: Schematische Darstellung Datennetz SBB[1]

Durch diese Trennung können sich Störungen oder Änderungen aus dem Anschlussnetz für Büroanwendungen (schwarz) theoretisch nicht im Anschlussnetz für bahnbetriebskritische Systeme (rot / grün) auswirken.

1.2 Prüfungsziel und -fragen

Ziel der Prüfung ist, zu untersuchen ob das neue Datennetz zweckmässig und sicher ist. Die Prüffragen lauten:

1. Ist das Design der neuen Netzinfrastruktur so konzipiert, dass eine angemessene Sicherheit (Verfügbarkeit, Vertraulichkeit, Integrität) und Resilienz erreicht wird?
2. Besteht ein angemessenes Risiko- und Qualitätsmanagement für das Programm und die technische Umsetzung?
3. Läuft das Projekt inhaltlich, zeitlich und kostenmässig nach Plan?

Der Fokus zu diesen Fragen richtet sich hauptsächlich auf die für den Bahnbetrieb kritischen Netzwerke. Das Zugsteuerungssystem European Train Control System (ETCS), das Kommunikationsnetz GSM-Rail sowie das Anschlussnetz für Büroanwendungen und bahnbetriebsnahe Systeme sind nicht Gegenstand der Prüfung.

[1] Grafik SBB I-AT-TC, 29. März 2017

1.3 Prüfungsumfang und -grundsätze

Die Prüfung konzentrierte sich auf das Anschlussnetz für bahnbetriebskritische Anwendungen der SBB AG. Sie erfolgte anhand der International Organization for Standardization (ISO) Standards 2700x sowie anhand des Minimalstandards zur Verbesserung der IKT-Resilienz des Bundesamtes für wirtschaftliche Landesversorgung (BWL).

IKT-Minimalstandard als Ausdruck der Schutzverantwortung des Staates

Der IKT-Minimalstandard des BWL dient als Empfehlung und mögliche Leitplanke zur Erhöhung der IKT-Resilienz. Er richtet sich vornehmlich an die Betreiber von KI, ist aber grundsätzlich für jedes Unternehmen anwendbar. Er kann als Nachschlagewerk dienen und vermittelt Hintergrundinformationen zur IKT-Sicherheit. Das Framework und das dazu gehörende Self-Assessment-Tool bietet den Anwendern, gegliedert nach den fünf Themenbereichen «Identifizieren», «Schützen», «Detektieren», «Reagieren» und «Wiederherstellen», ein Bündel konkreter Massnahmen zur Umsetzung an.

Der IKT-Minimalstandard setzt dort an, wo sich die Gesellschaft Ausfälle am wenigsten leisten kann: bei den IT-Systemen, welche für das Funktionieren der KI von Bedeutung sind. Betreibern von KI wird empfohlen, den vorliegenden IKT-Minimalstand oder vergleichbare Vorgaben umzusetzen.

Weiter kamen die Empfehlungen des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum IKT-Grundschutz zur Anwendung.

Die Prüfung wurde von Roland Gafner (Revisionsleiter) und Christian Brunner vom 12. August bis 19. November 2019 durchgeführt. Sie erfolgte unter der Federführung von Bernhard Hamberger. Die Ergebnisbesprechung hat am 15. Oktober 2019 stattgefunden. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Ergebnisbesprechung.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der Eidgenössischen Finanzkontrolle (EFK) von allen Beteiligten umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen sowie die benötigte Infrastruktur standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 19. November 2019 statt. Teilgenommen haben seitens der Geprüften der Leiter I-AT, der Leiter I-AT-TC, der stellvertretende Leiter I-AT-TC, der Technology Officer I-NAT, der Leiter Strategic Asset Management, die Leiterin I-AT-TC-TPP, der Leiter I-AT-TC-TEC-AR, der CISO und der Leiter IR. Das BAV wurde durch den Sektionschef Sicherheitstechnik vertreten. Seitens der EFK haben der zuständige Mandatsleiter, der Federführende und der Revisionsleiter mit einem Teammitglied teilgenommen.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung der Konzernleitung bzw. dem VR der SBB AG obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

2 Ein anfänglich unterschätztes Programm

2.1 Das Programm ist inhaltlich und zeitlich auf Kurs…

Die Umsetzung der Arbeitspakete im Programm entspricht den Planungsvorgaben. Es ist jedoch zu bemerken, dass sich in den vergangenen Jahren der Umfang und die Anforderungen erheblich verändert haben. Die rasante Entwicklung der Anforderungen an das Netz führte bis zum Abschluss des Programms «Datacom-NG» nahezu zu einer Verdopplung der Anzahl an Ports. Dies wurde bei der Erstellung des Pflichtenhefts im Jahr 2014 unterschätzt. Auch in Zukunft werden grössere Digitalisierungsvorhaben wie z. B. smartrail 4.0[2] dazu führen, dass das Datennetz eine immer wichtigere Rolle einnimmt. Um dieses Wachstum an Ports, Diensten und Datenmengen heute und in Zukunft beherrschen zu können, entwickelte die SBB AG im Rahmen des Programms neue Werkzeuge zur Automatisierung. Ein manueller Betrieb des Datennetzes wäre künftig ohne signifikanten Ressourcenaufbau oder Einbussen bei der Servicequalität nicht mehr möglich.

Seit Mitte 2017 ist der Rollout im Gang und zirka 80 % der Streckenabschnitte sind gebaut. Im ersten Quartal 2020 soll der Bau abgeschlossen werden. Ebenfalls sind rund 80 % des Datennetzes in Betrieb und werden aktiv durch das Operation Center Technik (OCT) überwacht. Die Migration der Dienste auf das neue Datennetz erwies sich als grosse Herausforderung. Besonders die Migration der Bahnhöfe stellte sich aufgrund der heterogenen Umgebung und der erhöhten Anforderungen als komplexes Vorhaben dar. Damit diesen Herausforderungen begegnet werden konnte, wurden Konzepte erarbeitet, um die Migration zu planen und entsprechend zu optimieren. Dadurch ist eine vernachlässigbare zeitliche Verschiebung bei der Migration und Automatisierung aufgetreten. Zum Prüfzeitpunkt sind rund 10 % der Dienste migriert. Dieser Rückstand soll durch die zunehmende Automatisierung der Migrationsprozesse eingeholt werden.

Grundsätzlich erachtet die SBB AG den Zeitfaktor in diesem Programm nicht als kritische Grösse. Die SBB AG legt wesentlich mehr Wert auf Qualität und Betriebssicherheit. In einem heute immer stärker verknüpften Bahnnetz muss grundlegend auf Qualität und Betriebssicherheit geachtet werden. Dennoch ist sich die SBB AG bewusst, dass ein Abschluss des Programms und somit auch der Rückbau der alten Infrastruktur zeitnah erfolgen muss. Zum einen ist eine allfällige Fehlersuche in einem parallel betriebenen Netz schwieriger, zum anderen verursacht der parallele Betrieb grosse Mehrkosten.

Beurteilung

Das Programm ist inhaltlich und zeitlich auf Kurs, die Programmziele können erreicht werden. Seit der Ausschreibung im Jahr 2014 haben sich sehr viele Änderungen ergeben, welche den ursprünglichen Fokus einer 1:1-Ablösung des Datennetzes etwas in den Hintergrund rücken lässt. Einerseits wurde zu Programmbeginn das Wachstum massiv unterschätzt, andererseits wurden zahlreiche zusätzliche Dienste und Aufgaben im Zuge der voranschreitenden Digitalisierung in das Programm integriert. Auf der Zeitachse sind die Folgen dieser Erweiterungen kaum spürbar, einzelne Projekte sind leicht in Verzug, aber diese sollen bis Ende Jahr wieder auf Kurs bzw. abgeschlossen sein.

[2] Mit dem Programm smartrail 4.0 nutzen die Schweizer Bahnen die Digitalisierung und das Potenzial neuer Technologien, um die Kapazität und die Sicherheit weiter zu erhöhen, die Bahninfrastruktur effizienter zu nutzen, Kosten zu sparen und damit die Wettbewerbsfähigkeit der Bahn längerfristig zu erhalten.

2.2 … aber Umfang und Kosten wurden massiv unterschätzt

Der VR der SBB AG hat anlässlich der Sitzung vom 9. Mai 2014, die Erneuerung des Datennetzes der SBB AG mit einer Gesamtinvestition von 155 Millionen Franken (+/- 30 %, Preisbasis 01/2014) beschlossen. Darin integriert ist der Werkvertrag mit dem externen Dienstleister und Lieferanten, welcher mit 100 Millionen Franken veranschlagt wurde. Die Mittel werden über die Fachbereiche finanziert. Die dezentrale Verwaltung der Finanzen in den Regionen hat sich im Laufe des Programms als nicht optimal erwiesen. Daher ist das Budget nun in der Verantwortung des Programmmanagers. Die Projekte haben entsprechend der identifizierten Arbeitspakete ein definiertes Budget, das laufend überprüft wird. Mitte 2018 wurde das Kostendach auf 185 Millionen Franken erhöht. Aktuell sind im Programm Kosten von rund 160 Millionen Franken aufgelaufen. Zurzeit wird ein weiterer Nachtrag zur Erhöhung des Kostendachs an den VR ausgearbeitet. Mit diesem soll das Portfolio auf 250 bis 275 Millionen Franken aufgestockt werden, damit die weiter anfallenden Kosten bis zum Programmende gedeckt werden können. Die Kosten liegen somit deutlich über dem geplanten Budget aus dem Jahr 2014. Im ursprünglichen Programmauftrag waren lediglich Kosten für die Migration des damaligen Bestandes-Netzes ausgewiesen (1:1-Migration). Zwischenzeitlich hat sich das Netz massgeblich erweitert. Die Bereitstellung dieser Weiterentwicklungen erfolgte ebenfalls durch das Projektteam. Dabei wurden die finanziellen Aufwände für diese teilweise auch fälschlicherweise dem Programm zugeordnet. Die finanzielle und organisatorische Situation wird nun aufgearbeitet. Ein durch den Leiter der Division Infrastruktur in Auftrag gegebenes Audit soll hier Klarheit schaffen. Erwartet wird eine Prognose zur Kostensituation am Programmende. Zudem werden Empfehlungen zu sinnvollen Rahmenbedingungen erwartet, um den Anforderungen von IKT-Projekten in der Division Infrastruktur besser gerecht zu werden.

Beurteilung

Die Kostenentwicklung übersteigt den ursprünglich geplanten Aufwand erheblich. Sie entspricht nahezu einer Verdoppelung der Kosten. Da zu Beginn des Programms die individuellen, relevanten Steuergrössen nicht definiert wurden, kam es erst zu einem späten Zeitpunkt zu der nötigen finanziellen Transparenz. Für ein Projekt dieser Grösse ist ein finanzielles Controlling erforderlich, welches die Entwicklung der Kostentreiber transparent darstellt. Die Programmdauer von mehreren Jahren, bedingt eine hohe Transparenz und Messbarkeit der relevanten Steuergrössen.

Die SBB AG hätte die fehlerhaften Kostenzuordnungen laufend erkennen und bereinigen können. Im Rahmen des Programms «Datacom-NG» wurden die Controllingmechanismen inzwischen verbessert (Stand September 2019). Es sind inzwischen Werkzeuge vorhanden, damit die Kosten pro Arbeitspaket erfasst und so eine möglichst exakte Prognose des Mittelbedarfs bis Programmende erstellt werden kann. Diese Mechanismen wurden jedoch zu einem sehr späten Zeitpunkt im Programm eingeführt. Die angeordnete Aufarbeitung der finanziellen Situation mittels eines Audits scheint in diesem Fall eine angemessene Massnahme. Der Bericht soll Ende Oktober 2019 vorliegen. Eine Würdigung der Ergebnisse durch die EFK ist somit im Rahmen der vorliegenden Prüfung nicht mehr möglich. Es bleibt offen, ob der Lenkungsausschuss seine Rolle und Verantwortung bezüglich der finanziellen Entwicklung wahrgenommen hat oder basierend auf den verfügbaren Informationen gar nicht wahrnehmen konnte.

Empfehlung 1 (Priorität 1)

Um in künftigen IKT-Programmen und -Projekten lückenlose und transparente Informationen hinsichtlich der finanziellen Ressourcen erhalten zu können, empfiehlt die EFK der SBB AG ein sinn- und zweckgerichtetes Controlling der Kosten zu etablieren und durchzusetzen. Das Controlling soll in eine zweckmässige Projektmanagementmethodik eingebunden werden (siehe Empfehlung 2).

Stellungnahme des Geprüften

Die ab 2020 gültige Systematik der finanziellen Führung des Programms wird im Januar 2020 durch den Lenkungsausschuss Datacom-NG verbindlich freigegeben werden. Der Lenkungsausschuss übernimmt die Verantwortung für die konsequente Umsetzung. Die Empfehlungen der EFK zum Controlling von Programmen und Projekten im IKT-Umfeld werden im Projektmanagement-Handbuch der übergeordneten Organisation (Telecom) aufgenommen und umgesetzt.

2.3 Eine ungeeignete Projektmanagement-Methode belastet das Programm

Das Programm wurde ursprünglich von einem internen Mitarbeiter der SBB AG geleitet. Seit 2018 wird die Rolle des Programmleiters durch eine externe Person wahrgenommen. Diese steuert die verschiedenen Projekte im Rahmen des Programms und koordiniert die Zusammenarbeit mit dem externen Leistungserbringer. Das Programm ist in einer Matrixorganisation aufgebaut. Die Fachbereiche haben eine koordinierende Rolle mit den Kunden schweizweit und sind verantwortlich, dass die Querschnittsprojekte (Konzepte, Rollout-Netz, Migration und Betrieb) ihre Aufgaben termingerecht erfüllen können. Die Zusammenarbeit im Programm wird von allen Projektleitern und den Vertretern der externen Firma als sehr konstruktiv und zielführend beurteilt. Die Programmführung wird als kompetent und angemessen wahrgenommen. Die Aufgaben und Verantwortlichkeiten sind geregelt und teilweise niedergeschrieben (z. B. Migrationshandbuch, Werkvertrag usw.). Der Austausch zwischen den einzelnen Projekten und der Programmleitung ist intensiv und erfolgt über verschiedene regelmässige Meetings. An diesen wird u. a. der Ressourceneinsatz und die Priorisierung der Arbeiten definiert. Der Lenkungsausschuss wird im Rahmen von regelmässigen Meetings und mittels eines monatlichen Reportings über den Stand des Programms informiert.

Die Projektmanagement-Methode der Division Infrastruktur ist für IKT-Programme ungeeignet

Die Projekte in der Division Infrastruktur werden primär nach den Normen des SIA für Bauprojekte geführt. Der Bereich Telecom kann angesichts der sich rasch wandelnden Charakteristik und Anforderungen an das Projektmanagement nicht mit diesen Methoden arbeiten. Komplexe IKT- und Netzwerkprojekte können nicht mehr ausschliesslich mit einer klassischen Methode abgewickelt werden. Im Programm «Datacom-NG» kommt daher keine einheitliche Projektmanagement-Methode zur Anwendung. Einige Projekte arbeiten sehr agil, andere wiederum können mit klassischen Wasserfallmethoden abgewickelt werden (z. B. Rollout). Für das Management derartiger Programme und Projekten existieren im Gegensatz zu klassischen Bauprojekten für Telecom keine Vorgaben. Der Programm- und

die jeweiligen Projektleiter sind in der Wahl der Methode frei. Daher ist auch nicht vorgegeben, welche Lieferobjekte und Werkzeuge zum Einsatz kommen. Dies führt u. a. dazu, dass die Projektleiter erst Werkzeuge für die Projektführung entwickeln müssen. Das Programm und die Teilprojekte werden weitgehend über Dokumente und Meetings geführt. Bei den Projektleitern wird jedoch grosser Wert auf Zertifizierungen im Bereich Projektmanagement gelegt.

Es existieren Prozesse und Handlungsempfehlungen, die sich an die Methode Hermes 5 anlehnen, diese waren aber zum Prüfzeitpunkt nicht verbindlich. Nach der Verabschiedung des Prozesses und der Veröffentlichung im Prozessmanagement-Tool sollen diese Abschnitte dann verbindlich zur Anwendung kommen.

In einer externen Untersuchung vom 29. September 2016 wurde überprüft, ob das Programm für eine zielorientierte Umsetzung bereit war. In diesem Expertenbericht wurde damals festgestellt, dass das Projektmanagement ohne vereinheitlichte Vorgaben aus unterschiedlichen Gründen nicht optimal ist. Die Empfehlung hierzu lautete: «SBB I-AT-TC sollte für das Programm- und Projektmanagement einen Standard definieren. Die Verwendung einer Projektmanagement-Plattform würde dies unterstützen. »

Die Bedeutung der IT-Integration in Bauprojekten nimmt zu

Die Technisierung und Automatisierung in Gebäuden und Infrastrukturen nimmt stetig zu. Intelligente Gebäudesteuerungen erlauben, Verbindungen zwischen den verschiedenen Techniken, der Elektronik, Physik, Automatisierung, Informatik und Telekommunikation in einem Gebäude oder einer Anlage herzustellen. Um den zukünftigen Anforderungen gerecht zu werden, müssen organisatorische Anpassungen bei der Planung, im Bau und innerhalb des Objektmanagements vollzogen werden.

Als Grundlage für Bauprojekte kommen heute vorwiegend die Normen des SIA zum Tragen. Diese Vorgehensweise ist sehr phasenorientiert und nimmt in der Regel einen längeren Zeithorizont in Anspruch. IT-Projekte und im Besonderen Entwicklungsprojekte weisen hingegen wesentlich kürzere Zyklen auf. Diese agile Arbeitsweise kann nicht ohne Weiteres in der Methodik des SIA abgebildet werden. Längerfristig muss eine Lösung gefunden werden, damit die beiden Bereiche in enger Abstimmung gemeinsame Projektziele erreichen können.

Beurteilung

Grundsätzlich sind das Programmmanagement und die Organisation heute gut aufgestellt. Seit dem Wechsel des Programmleiters 2018 sind zahlreiche Optimierungsmassnamen zur Steuerung des Programms vorgenommen und neue Werkzeuge entwickelt worden. Dennoch fehlt aus Sicht der EFK eine einheitliche Methodik im Programm und in den Projekten. Eine solche ist für eine effiziente Führung und das lückenlose Controlling unabdingbar. Protokolle, Pendenzen und Entscheide werden vom Programmleiter und von den Projektleitern in eigenen Werkzeugen festgehalten. Dies erscheint wenig geeignet für Projekte mit zahlreichen Interdependenzen und schafft starke Abhängigkeiten von Schlüsselpersonen.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt der SBB AG für künftige Vorhaben an der Schnittstelle von digitalen/IKT- und klassischen / SIA-Projekten, in Abstimmung mit den übergeordneten Vorgaben, eine Methodik für Projekte und Programme vorzugeben. Dabei sollen Anforderungen resp. Möglichkeiten der zunehmenden Digitalisierung antizipiert und den agilen Methoden Rechnung getragen werden.

Stellungnahme des Geprüften

Die Empfehlungen der EFK zur Führung von hybriden Projekten mit IKT- und SIA-Anteilen, in Abstimmung mit übergeordneten Vorgaben, eine Methodik für Projekte und Programme vorzugeben, wird im Verlaufe 2020 umgesetzt. Diese Vorgaben werden im Projekt Data-com-NG konsequent angewendet.

3 Das Risiko- und Qualitätsmanagement sollte verbessert werden

3.1 Die fehlende Unabhängigkeit im Risiko- und Qualitätsmanagement wurde adressiert

Das Risikomanagement (RM) ist ein fester Bestandteil im Programm und den Projekten. Dabei ist das RM einem dauernden Zyklus für die periodische Risikobeurteilung unterworfen. Es werden sowohl Output-Risiken (Projektrisiken) als auch Risiken aus dem Umfeld des Programms (Kollateral-Risiken) erfasst und behandelt. Vom Konzern bzw. der Division Infrastruktur sind verschiedene Vorgaben zum Risikomanagement vorhanden. Die «Ausführungsbestimmungen Risikomanagement Infrastruktur» legen die Ziele, den Anwendungsbereich, den Prozess und den Aufbau (inkl. Aufgaben, Kompetenzen, Verantwortung) für die Division Infrastruktur fest. Für Programme und Projekte werden die Anforderungen in den «Ausführungsbestimmungen Risikomanagement in Projekten» detaillierter spezifiziert. Die Vorgaben sind für sämtliche Programme und Projekte unter der Leitung der Division Infrastruktur verbindlich. Die Verantwortung für die korrekte Umsetzung obliegt dem Projekt-/Programmleiter, Gesamtprojektleiter oder Fachbauprojektleiter.

Seit dem Programmstart im Jahr 2014 wurde das Risiko- und Qualitätsmanagement (QM) durch den stellvertretenden Auftraggeber und Mitglied des Lenkungsausschusses wahrgenommen. Eine dedizierte bzw. unabhängige Rolle hierfür fehlte. Die SBB AG erkannte, dass dies im Rahmen des Programms nicht optimal ist und hat eine entsprechende Stelle geschaffen. Diese konnte am 1. September 2019 durch einen neuen Mitarbeiter besetzt werden, der für das gesamte RM und die Qualitätssicherung (QS) zuständig ist, also auch in den einzelnen Projekten. Die Unterstellung ist bei der Leiterin I-AT-TC-TPP, wodurch die Unabhängigkeit gegenüber der Programmorganisation gewährleistet ist.

Beurteilung

Die Doppelrolle als stellvertretender Auftraggeber und Beauftragter für das RM und die QS in einer Programm-/Projektorganisation ist zu vermeiden. Eine unabhängige Berichterstattung an den Lenkungsausschuss kann nicht durch ein Mitglied in einer Doppelrolle wahrgenommen werden. Die SBB AG hat dies zwar erkannt, jedoch zu einem späten Zeitpunkt im Programmverlauf reagiert. Mit der Schaffung einer neuen und unabhängigen Stelle hat die SBB AG diesem Umstand entgegengewirkt und die Organisation in einem wesentlichen Bereich verstärkt. Das geplante inhaltliche Vorgehen des neuen Risiko- und Qualitätsmanagers erachtet die EFK als zielführend. Aus diesem Grund verzichtet sie auf eine Empfehlung.

3.2 Risikoerhebung und Rapportierung sollten verbessert werden

Zu Programmbeginn wurden initial fünf Hauptrisiken (Risikokategorien) mit jeweils unterschiedlichen Teilrisiken ermittelt. Diese adressieren im Wesentlichen den Betrieb, die Migration und die Servicequalität. Die Risiken wurden detailliert in einem Projektrisikobericht zusammengefasst. Zur laufenden Aktualisierung und Identifikation der Risiken werden in Workshops neue, respektive geänderte Risiken erfasst und behandelt. Dort werden auch die Unternehmens- und finanziellen Risiken integriert. Halbjährliche "Risk Reviews" dienen der vertieften Risikoanalyse. In diesen nehmen die Fachexperten eine Coachingfunktion

wahr und sensibilisieren die Teams, damit ein kontinuierliches Risikomanagement etabliert werden kann. Diese Risiken werden in einem periodischen Statusbericht, dem «Programm Cockpit TC», dargestellt und an die übergeordneten Stellen kommuniziert. Die Angaben stammen aus unterschiedlichen Werkzeugen und werden an den Meetings besprochen und konsolidiert. Zudem müssen dem BAV gemäss Leistungsvereinbarung jährlich die Liste der Projekte mit erheblichen Risiken zugestellt werden. Dies erfolgte am 30. August 2019 das letzte Mal.

Für die Erfassung der für die Steuerung unerlässlichen Angaben zum Programm steht jedem Programmanager das Werkzeug «Navigator» zur Verfügung. Der Navigator ist Bestandteil des Enterprise-Resource-Planning (ERP) -Systems und stellt ein wesentliches SAP-Tool des Projekt- und Risikomanagements bei Infrastrukturprojekten dar. Mit dem Navigator werden wichtige Steuerungsgrössen zusammengefasst und bewertet sowie Ursachen und Massnahmen dazu dokumentiert. Neben Qualität / Leistung, Terminen und Kosten werden auch die Risiken auf Projektebene im Navigator bewirtschaftet. Die Verwendung des Navigators in Projekten mit einer Grössenordnung ab 10 Millionen Franken ist verbindlich. Initial wurden gewisse Projektphasen im Navigator abgebildet. Es hat sich jedoch gezeigt, dass das Instrument für das Bewirtschaften von Programmrisiken ungeeignet ist. Die Risiken wurden daher nicht mehr weiter in diesem Werkzeug gepflegt. Da keine einheitlichen Vorlagen oder Werkzeuge für die Erfassung und Behandlung von Programmrisiken existieren, erarbeiteten sich die Programmleiter eigene Werkzeuge, was die Aggregation bzw. Konsolidierung der Risiken erschwerte.

Beurteilung

Ein wirkungsvolles und abgestimmtes Risikomanagement in Programmen ist die Grundlage für ein erfolgreiches Risikomanagement auf Portfolioebene, d. h. die übergeordnete Sicht auf mehrere Projekte. Damit relevante Projektrisiken auch auf Stufe Division sowie auf Konzernstufe Beachtung finden, muss die Überführung der Projektrisiken in ein geeignetes Werkzeug gewährleistet sein. Die Lenkung von Programmen und Projekten durch die übergeordneten Stellen wird ohne einheitliche Werkzeuge bzw. Methoden erschwert.

Empfehlung 3 (Priorität 1)

Die EFK empfiehlt der SBB AG für künftige Programme, in Abstimmung mit den übergeordneten Vorgaben, eine einheitliche Methodik zur Behandlung und Rapportierung von Risiken sicherzustellen (siehe Empfehlung 2).

Stellungnahme des Geprüften

Seit September 2019 ist ein Risikomanager im Programm Datacom-NG tätig, der die regelmässige Bewertung der Risiken des Programms und deren Aktualisierung, sowie entsprechendes Reporting im übergeordneten Gremium und ins zentrale Risk Reporting der SBB und ins BAV sicherstellt. Die SBB AG sieht eine Überprüfung der Grundlogik und Prozesse insbesondere für IKT-Programme mit hybridem Charakter (SIA-Anteile) vor, um sicherzustellen, dass alle relevanten Risiken und deren Treiber auf den Risikoreportings der der Division Infrastruktur erscheinen.

4 Aktive Steuerung von der Planung zum Betrieb

4.1 Eine zukunftsgerichtete Architektur mit Fokus auf hohe Verfügbarkeit

Das Netzwerk umfasst das optische Transportnetz (OTN) sowie die übergeordneten Multi Protocol Label Switching (MPLS) -Netze Business-Data, Rail-Data und das Time-division Multiplexing (TDM)-Legacy-Netz (Synchrone Digitale Hierarchie, SDH). Die korrespondierenden Netze sind physisch bzw. auf dem optischen Layer durch verschiedene Kanäle getrennt und verfügen über redundante Wegeführungen (vgl. Abbildung 1: Schematische Darstellung Datennetz SBB). Eine Erhöhung der Bandbreite auf 100 Gigabit Ethernet (GE) ist vorgesehen und bei Bedarf realisierbar.

Die Netzwerke berücksichtigen die zukünftigen Anforderungen von IPv6. Ab 2020 soll die Kommunikation zwischen den neuen Zügen und der zentralen IT-Infrastruktur der SBB IT, End zu End IPv6 Native erfolgen.

Beurteilung

Die Architektur des neuen Netzwerkes ist grundsätzlich nachvollziehbar und erfüllt die Anforderungen an eine komplexe Kommunikationsinfrastruktur. Das Netz ist auf eine hohe Verfügbarkeit und Resilienz ausgerichtet, was für den sicheren Bahnbetrieb unabdingbar ist. Durch die eingesetzte Technologie und deren Konfiguration verfügt das Netz über eine gute Skalierbarkeit. Künftige Anforderungen, wie die Erhöhung der Bandbreite oder die Implementierung von IPv6, sind realisierbar.

4.2 Nicht alle Elemente der Sicherheitsarchitektur wurden gemäss Pflichtenheft umgesetzt

Die gängigen Mechanismen und Werkzeuge zur Absicherung der Netzwerke sind weitgehend implementiert. Firewalls schützen die internen Netzübergänge sowie die Kommunikation nach aussen. Intrusion-Detection-Syteme (IDS) und Intrusion-Prevention-Systeme (IPS) überwachen den Datenverkehr an Zonenübergängen, alarmieren bei Anomalien und blockieren unerlaubten Verkehr.

Beurteilung

IDS und IPS überwachen und analysieren die Aktivitäten im Netzwerk. Die Systeme können typische Angriffsmuster erkennen, abnormale Aktivitätsmuster analysieren und Verletzungen von Richtlinien erkennen. Zum Prüfzeitpunkt sind noch nicht alle Anforderungen aus dem Pflichtenheft umgesetzt. Mit dem Einsatz dieser Systeme wird ein wesentlicher Grundschutz im Netz erreicht.

Empfehlung 4 (Priorität 1)

Die EFK empfiehlt der SBB AG, die Vorgaben für die Implementierung der Sicherheitsvorkehrungen entsprechend dem Pflichtenheft im Rahmen des laufenden Projektes für alle Netze zu realisieren.

Stellungnahme des Geprüften

Die Schutzmassnahme ist technisch vorbereitet und wurde in Absprache mit Vertretern der Telecom, Sicherungsanlagen und dem BAV zur Vermeidung von damit verbundenen Risiken vorerst verschoben. Die Betriebsprozesse bei Operations Center Technik, Telecom und Sicherungsanlagen müssen diesbezüglich validiert (Erledigungstermin=Validierungstermin) werden. Nach erfolgreicher Validierung wird die Implementierung vorgenommen. Dies sollte im Verlaufe 2020 umgesetzt werden können.

4.3 Herausforderungen in der Umsetzung und Automatisierung werden aktiv angegangen

Die Prozesse im Rollout werden laufend optimiert

Das Rollout-Konzept beschreibt die Prozessschritte und Vorgaben zur Umsetzung der Infrastruktur im Projekt «Datacom-NG». Darin ist detailliert ausgeführt, nach welchem Drehbuch und welchen Grundprinzipien der Rollout schweizweit abläuft. Für die Erarbeitung des detaillierten Rollout- und Migrationsplans wurden die betroffenen Stellen der SBB AG eng eingebunden. Der Rollout umfasst die Bereitstellung der Basisinfrastruktur (Schränke, Stromversorgung, Verkabelung) sowie die Netzwerkkomponenten für das optische Transportnetz, das MPLS-Netz (Business Data & Rail-Data) sowie das TDM-Legacy-Netz.

Für die initiale Konfiguration zur Inbetriebnahme werden Basiskonfigurationen über den Verteilserver des Lieferanten aufgespielt. Dieser ist auch für die Erstellung, Qualitätssicherung und Verteilung der Basiskonfigurationen verantwortlich. Nach erfolgreichen mehrstufigen Tests und einem Probebetrieb gehen die Netzelemente in die Verwaltung des Betriebes über, welcher dann für die betriebsbedingte Netzkonfiguration verantwortlich ist. Für die Automatisierung und Optimierung des Rollouts mithilfe von Prozessdigitalisierung und -visualisierung wurden neue Wege beschritten. Die Komplexität und die Umsetzung der Auflagen nach CENELEC und des BAV generierten einen hohen Aufwand.

Zahlreiche Konzepte regeln die Migration der Services auf das neue Netz

Das Migrationsprojekt ist als Folge zum Rollout-Projekt zu sehen und realisiert die Migration der bestehenden Anwendungen und Telecom-Services im laufenden Betrieb. Hierfür wurde ein «High-Level Migrationskonzept» erstellt, welches die Gesamtplanung zur Migration beschreibt, insbesondere die Grundprinzipien, die Migration der bestehenden Anwendungen und Services sowie die Migrationsstrategien der wichtigsten Plattformen. Die spezifischen Detailkonzepte beinhalten plattform- und anwendungsspezifische Aussagen zur Migration wie z. B. Dokumentation des aktuellen Zustands, Randbedingungen für die Migration, Migrationsvorgehen, Migrationsplanung und das entsprechende Drehbuch. Die wichtigsten Anwendungen und Plattformen sind klassifiziert in sicherheitsrelevante Anwendungen, nicht sicherheitsrelevante aber bahnkritische Anwendungen und nicht sicherheitsrelevante aber bahn-, kunden- oder mitarbeiternahe Anwendungen.

Die grösste Herausforderung stellt die extrem heterogene Netz- und Legacy-Konfiguration dar. Technische Probleme sind schwer zu antizipieren, daher versucht die SBB AG diese mit Handlungsanweisungen basierend auf Erfahrungen zu mitigieren.

Beurteilung

Das Rollout-Projekt ist aus Sicht der EFK professionell aufgesetzt und der Fortschritt in Übereinstimmung mit der Planung. Die mehrfache Überprüfung der Basiskonfigurationen zur Sicherstellung der Funktionalität erachtet die EFK als sinnvoll. Trotz knapp bemessener Ressourcen ist das Projekt «Rollout» in der Lage, die Voraussetzungen für die Migration zu schaffen.

Die Migration stellt einen sehr komplexen Teil des Programms dar. Die Überführung der zahlreichen und heterogenen Services stellt die SBB AG vor eine grosse Herausforderung. Die EFK erachtet das Vorgehen bei der Migration und den hohen Grad der Automatisierung als zielführend.

4.4 Ein störungsfreier Betrieb hat oberste Priorität

Die wichtigsten Anforderungen an den Betrieb sind, das Netz und die darauf realisierten Services möglichst störungsfrei zu betreiben. Durch die Automatisierung wird die Effizienz gesteigert, die Kundenorientierung verbessert und ein umfassendes Monitoring sowie Reporting gewährleistet. Die Überwachung des Datennetzes wird präventiv und reaktiv sichergestellt und erfolgt innerhalb des OCT im 7x24 Stunden Betrieb.

Die Betriebsmanagementsysteme sind redundant aufgebaut. Der Zugang wird personifiziert und aufgabenspezifisch abgesichert. Der Lieferant ist an das Incident-Managementsystem direkt angebunden und erhält dadurch die notwendigen Informationen für allfällige Interventionen.

Neue Konfigurationen werden vom Telecom-Engineer erstellt, dem Betrieb übergeben und von zwei Mitarbeitenden des Betriebs vorgängig zur Implementierung kontrolliert. Die Implementierung erfolgt im Vier-Augen-Prinzip. Die Konfigurationen der Netzelemente werden im Network Management System (NMS) abgespeichert. Die Service Bereitstellung soll durch die Fulfillment-Factory (FFF) vollständig automatisiert werden. Diese befand sich in der Einführungsphase.

Eingriffe in die Konfiguration der Netzelemente und Sicherheitselemente (z. B. Firewalls) werden detailliert protokolliert und überwacht. Eine Rückverfolgung der Änderungen sowie die Herstellung alter Zustände sind gewährleistet. Der Zugang zu den Netzelementen kann nur im internen geschlossenen SBB-Daten-Netz erfolgen.

Im Konzept zum Backup und Restore der Kommunikationsinfrastruktur sind die gerätespezifischen Anforderungen detailliert beschrieben. Die Datensicherung erfolgt regelmässig. Tests zur Datenwiederherstellung werden bei der Inbetriebnahme durchgeführt und unterliegen keinem dauernden Prozess. Wenn im Falle eines Incidents die Wiederherstellung funktioniert, wird auf weitere Tests verzichtet.

BCM und Krisenmanagement sind etabliert, die Konzepte müssen noch mit den neuen Anforderungen aus dem Programm «Datacom-NG» ergänzt werden. Der technische Betrieb verfügt über eine Notfall-Stabsorganisation. Im Falle von gravierenden Störungen werden entsprechend der Schwere der Störung sofortige Interventionen umgesetzt bzw. der Notfall-Stab aufgeboten.

Beurteilung

Die Systeme und Prozesse sind mit einer hohen Verfügbarkeit und Resilienz implementiert. Einige Prozesse sind derzeit noch im Aufbau bzw. die Dokumentationen werden noch vervollständigt. Die betriebliche Organisation ist auf einem hohen Niveau.

Die FFF funktioniert zuverlässig, dennoch gibt es teilweise noch Probleme mit der Datenqualität. Dieses Thema ist durch die SBB AG erkannt und entsprechend in Bearbeitung.

Die SBB AG ist sich der Wichtigkeit des Backups bewusst und hat solche konzeptionell auch angemessen umgesetzt. Allerdings wird die Wiederherstellung der Daten aus dem Backup nicht systematisch und regelmässig geprobt. Nur mittels regelmässiger Tests der Datenwiederherstellung kann sichergestellt werden, dass im Störfall auf erprobte Prozesse zurückgegriffen werden kann und diese auch funktionieren.

BCM und Krisenmanagement sind gut etabliert, regelmässige Übungen und Tests der Notfallbearbeitung werden durchgeführt. Die Anpassung der Konzepte mit den neuen Gegebenheiten wurde als Pendenz dokumentiert.

Empfehlung 5 (Priorität 2)

Die EFK empfiehlt der SBB AG, Tests im Rahmen der Wiederherstellungsverfahren zum Netzwerkmanagement zu planen und regelmässig durchzuführen.

Stellungnahme des Geprüften

Die regelmässige Überprüfung (Tests) der Wiederherstellungsverfahren ist zwischenzeitlich in die Betriebsplanung eingeflossen. Sie wird ab 2020 umgesetzt.

5 Den Vorgaben zur Sicherheit und Resilienz wird ein hoher Stellenwert beigemessen

5.1 Die konzernweiten Sicherheitsvorgaben und -verfahren weisen eine angemessene Maturität auf

Die konzernweiten Vorgaben zur Informationssicherheit werden vom Chief Information Security Officer (CISO) verantwortet und unterliegen einem steten Überarbeitungsprozess. Die Weisungen sind allen Mitarbeitenden zugänglich. Zur Zeit der Prüfung läuft der Prozess zur Zertifizierung des Information Security Management System (ISMS) nach DIN ISO/IEC 27001:2013. In einer ersten Phase wird die Zertifizierung im Kontext von «Datacom-NG» erst das Business-Netz umfassen. Eine Ausweitung auf die übrigen Netze und Dienste im Konzern ist in einem weiteren Schritt vorgesehen.

Vorgaben zur physischen Sicherheit sind Bestandteil der Konzepte

Die Vorgaben zur physischen Sicherheit werden durch die Corporate Security erlassen und sind für alle Projekte verbindlich. Die Vorgaben werden in den Konzepten des Programms entsprechend abgehandelt. Im Security-Konzept wird definiert, in welcher Schutzzone welches System eingebaut werden soll. Daraus ergeben sich die minimalen Anforderungen an bauliche und technische Sicherheitsmassnahmen für die Gebäude und Anlagen der SBB AG. Die Netzwerkkomponenten stehen in unterschiedlichen Schutzzonen. Entsprechend der Schutzzone wird auch der Zutritt festgelegt. Die Berechtigungen für die Zutritte laufen zentral über das Service Center Zutritt (SCZ). Diese sind mit dem SAP verknüpft, damit bei einem Austritt alle Zutritte wieder gelöscht werden. Letztere werden jährlich überprüft. Im Programm werden die Zutritte mittels Schlüssel und den entsprechend benötigten Rollen freigeschaltet. Die Zutritte werden sowohl auf dem Schlüssel sowie auch in einem Managementsystem aufgezeichnet, protokolliert und überwacht.

Die Räume mit aktiven Netzwerkkomponenten sind klimatisiert, die Stromversorgungen sind redundant erschlossen und verfügen über eine unterbrechungsfreie Stromversorgung (USV). Diese können die Standorte für vier Stunden autonom betreiben, was für die Überbrückung der häufigsten Stromunterbrüche ausreicht. Die Räume werden mittels Feuer- oder Rauchmelder und Alarmanlagen überwacht, geeignete Handfeuerlöscher sind auch vorhanden.

Die Umsetzung sollte im Programm stärker überprüft werden

Der CISO war zu Programmbeginn bei der Erstellung der Sicherheitskonzepte eng eingebunden. Im Wesentlichen hat der Bereich Information Security & Risk Management (IT-SR) die Qualitätskontrolle durchgeführt und die Anforderungen präzisiert. Periodische Prüfungen des Programms hinsichtlich der Einhaltung der Sicherheitsvorgaben sind keine vorgesehen. Grundsätzlich prüfen IT-SR bei Vorhaben ausschliesslich Dienste, welche in den Betrieb überführt werden hinsichtlich der Umsetzung der Sicherheitsvorgaben. Die Umsetzung allfälliger Massnahmen aus diesen Prüfungen werden entsprechend auditiert. Ein Audit über das gesamte Programm ist in der ersten Jahreshälfte 2020 geplant.

Beurteilung

Die Vorgaben sind sehr umfangreich und in einer hohen Qualität vorhanden. Zudem unterliegen sie auch einem periodischen Überarbeitungszyklus und sind entsprechend aktuell. Durch die Zertifizierung des ISMS nach DIN ISO/IEC 27001:2013 und der damit verbundenen jährlichen Überprüfungen wird zudem sichergestellt, dass auch künftig eine hohe Maturität gewährleistet bleibt.

Bezüglich Vorgabenumsetzung im Bereich der physischen Sicherheit konnte sich die EFK anlässlich eines Besuches einer umgebauten Anlage ein Bild verschaffen. Die besuchte Anlage ist vor unbefugtem Zutritt angemessen geschützt und der Zugang wird elektronisch protokolliert. Die Systeme werden durch unabhängige Stromquellen versorgt und sind bei einem Ausfall zudem durch eine USV geschützt. Die Absicherung der Räumlichkeit entspricht den Anforderungen der SBB AG an die physische Sicherheit.

Die Überprüfung der Sicherheitsanforderungen erfolgt nicht zeitgerecht. In einem Programm mit so zahlreichen neuen Anforderungen und Änderungen empfiehlt es sich, die IT-Sicherheit periodisch durch eine unabhängige Stelle prüfen und beurteilen zu lassen. Allfällige neue Anforderungen respektive notwendige Massnahmen können so zeitnah definiert und umgesetzt werden. Dies verhindert die Gefährdungen im Programm und Zusatzkosten wegen notwendiger Anpassungen am Ende des Programms.

Empfehlung 6 (Priorität 1)

Die EFK empfiehlt der SBB AG, bei längerfristigen Vorhaben die Einhaltung von Sicherheitsvorgaben und -konzepten, im Verlauf des Projektes periodisch zu prüfen. Dies insbesondere bei Abweichungen von den ursprünglich genehmigten Konzepten.

Stellungnahme des Geprüften

Die regelmässige Überprüfung von Systemen und Anlagen erfolgt zukünftig im Rahmen des ISMS und der zugehörigen Prozesse. Die Mittel dazu sind nebst den internen ISMS-Audits, die regelmässigen Risk Assessments, sowie die externen, periodischen Rezertifizierungen. Abweichungen von Vorgaben werden dabei erkannt und im Rahmen der Auditplanung vertieft überprüft. Im 2020 wird ein Gesamtaudit zur Informationssicherheit durchgeführt.

5.2 Mit dem Programm verbessert sich die Qualität des Inventars

Die Systeme im Kontext des Programms sind inventarisiert, das Inventar ist auf einem aktuellen Stand. Für den Rollout wurde eine Applikation für Mobilgeräte entwickelt. Mit dieser Applikation können sämtliche Daten inventarisiert und abgefragt werden. Das Inventar wird in zwei Systemen geführt und im Network-Function-Manager-Paket (NFM-P) abgebildet. Neue Netzelemente beziehen ihre Konfigurationen aus dem NFM-P und senden ihre Systemdaten wiederum an dieses zurück. Dadurch kann eine sehr hohe Konsistenz und Vollständigkeit der Daten erzielt werden.

Beurteilung

Um den Überblick zu behalten und um sicherzustellen, dass nur die gewünschten Systeme an das Netzwerk angeschlossen werden, ist ein korrektes lückenloses Inventarmanagement zwingend notwendig. Das Inventar der vom Programm betroffenen Systeme ist auf einem aktuellen Stand und wird durch die automatisierte Erfassung und Bearbeitung laufend verbessert. Somit ist sichergestellt, dass im Falle einer Störung die nötigen Informationen zur

Störungsbehebung vorhanden sind. Die EFK misst der korrekten Erfassung der Systeme im Inventartool einen hohen Stellenwert bei. Sie legt der SBB AG nahe, im Hinblick auf die Automatisierung von Unterhalt und Betrieb weiterhin stark auf eine hohe Qualität dieser Informationen zu achten.

5.3 Die Netzwerktrennung wird auch bei der Administration berücksichtigt

Die Administratoren verfügen für jedes Netz über ein gesondertes Benutzerkonto. Mit diesem melden sie sich am Netzelement bzw. am NMS an. Die Berechtigungen für den jeweiligen Nutzer sind durch Nutzergruppen definiert und bestimmen die Netzelemente, an denen ein Nutzer Änderungen vornehmen darf. Die entsprechende Dokumentation ist vorhanden. Die Authentifizierung ist mit Passwörtern und einem zentralen Authentifizierungsdienst abgesichert. Das Passwortkonzept ist zu überprüfen gemäss Mängelliste im Programm.

Beurteilung

Die physische Trennung der Netze wird auch bei der Zugriffs- respektive Berechtigungssteuerung konsequent umgesetzt. Damit wird verhindert, dass jemand ein «falsches» Element konfiguriert. Die entsprechenden Rollen dazu sind definiert und beschrieben.

Die Umsetzung weiterer Massnahmen zur Berechtigungssteuerung und Zugriffschutz sind bei der SBB AG in Planung, weshalb die EFK von einer Empfehlung absieht.

5.4 Die Handhabung von Sicherheitsvorfällen ist angemessen umgesetzt

Der Incident-Management-Prozess erfolgt nach dem Code of Practice ISO 27002. Die Anbindung der Systeme an das bestehende Operation Support System (OSS) und Security-Incident und Event Management System (SIEM) sind im SIEM Integrationskonzept beschrieben. Aufgabe des SIEM Systems ist es, sicherheitsrelevante Vorkommisse aufzuzeigen und zu alarmieren. Hierfür werden verschiedene Datenquellen eingebunden und ausgewertet. Die Alarme werden durch die Mitarbeitenden des OCT ausgewertet und die entsprechenden Störungstickets erstellt. Diese werden den zuständigen Bereichen zur Bearbeitung zugeteilt. Je nach Dringlichkeit werden Sofortmassnahmen ergriffen, respektive weitere Personen aufgeboten. Dadurch ist sichergestellt, dass bei Bedarf auch der Lieferant (Third Level Support) eingeschaltet werden kann. Der Lieferant unterstützt die SBB AG durch ein Computer Emergency Response Team (CERT) und ein Product Security Incident Response Team (PSIRT). Security Alarme und deren Lösungen (z. B. Security Patches) sollen zeitgerecht durch den Lieferanten zur Verfügung gestellt werden, sind eindeutig identifizierbar und klassifiziert. Die Informationsverteilung ist auf die inventarisierte Basis (Hardware und Software) der SBB AG angepasst. Reports werden vom Lieferanten zur Verfügung gestellt. Risiken, Auswirkungen und Lösungen werden in den Betriebsausschussmeetings mit den Partnern thematisiert. Die Überwachung der Verwundbarkeiten der eingesetzten Produkte wird durch das PSIRT des Lieferanten sichergestellt.

Beurteilung

Die Organisation und Umsetzung für die Behandlung von Sicherheitsvorfällen weist einen hohen Reifegrad aus. Ereignisse werden mittels verschiedener Werkzeuge aufgezeichnet und ausgewertet. Die Unterstützung durch den Lieferanten ist in die Supportkette eingebunden und zielführend definiert. Die Netzsysteme wurden ins bestehende SIEM integriert und Alarme werden dadurch bearbeitet. Der Prozess zur Behebung der Störungen ist dokumentiert, der Third-Level-Support sichergestellt und der Eskalationsprozess definiert.

Bei der Erkennung von Verwundbarkeiten der Infrastruktur verlässt sich die SBB AG auf den Lieferanten. Der Prozess sowie die Hilfsmittel zur aktiven Erkennung von Sicherheitsvorfällen und von Verwundbarkeiten existiert heute nur teilweise Daraus ergibt sich ein Risiko, dass bei Bekanntwerden einer Verwundbarkeit, die SBB AG auf die Reaktion des Lieferanten angewiesen ist und allfällige Sofortmassnahmen nicht zeitnah umsetzen kann.

Empfehlung 7 (Priorität 2)

Die EFK empfiehlt der SBB AG, für die eingesetzten Komponenten und Werkzeuge einen Prozess zur proaktiven Informationsbeschaffung bezüglich Verwundbarkeiten zu etablieren.

Stellungnahme des Geprüften

Das Programm «cyber@SBB» baut 2020 bis 2023 ein Cyber Defence Center (CDC) auf. Dieses wird in einer angemessenen Maturität aktiv die kritischen Anlagen und Systeme der SBB auf Schwachstellen und mögliche Angriffe überwachen und verstärkt die bisherigen etablierten Sicherheitsmassnahmen. Das angesprochene «Vulnerability Management» (VM) zu etablieren, wurde als wichtige Fähigkeit des CDC identifiziert und erste VM-Installationen laufen bereits seit Mitte 2019 im Bereich der Informatik. Im Bereich der Netzwerkelemente wird die SBB einen Prozess etablieren, um für die eingesetzten Komponenten und Systeme proaktiv zu Informationen bezüglich ihrer Verwundbarkeit zu gelangen (über Hersteller, andere Anwender, Marktinformationen, weitere).

5.5 Nicht detaillierte Vorgaben zur IT-Sicherheit

Um die Sicherheit von bahnkritischen Anlagen (Sicherungsanlagen) sicherzustellen, müssen alle sicherheitsrelevanten Änderungen an Anwendungen sowie dazugehörige Datennetze vom BAV bewilligt werden. Dies erfolgte für das Vorhaben der SBB AG mittels Zwischenverfügung vom 26. Juli 20172017 und Bewilligung zur Betriebserprobung vom 1. Juni 2018. Für jede weitere Anwendung muss in einem gesonderten Prozess die Eignung der gewählten Bauform des Datennetzes nachgewiesen werden. Zudem muss während der Betriebserprobungsphase eine Freigabe des BAV beantragt werden. Zum Prüfzeit-punkt haben sieben Anwendungen die «Freigabe für Probebetrieb», der mindestens drei Monate dauern muss. Die massgeblichen Vorgaben sind die Verordnung über Bau und Betrieb der Eisenbahnen (EBV) sowie die AB-EBV. Zudem gibt es verschiedene Standards (z. B. CENELEC EN 50126, EN 50128, EN 50129, EN 50159) sowie Richtlinien und Vorgaben, etwa die Richtlinie Typenzulassung für Elemente von Eisenbahnanlagen (RL TZL) oder die Richtlinie «Nachweisführung Sicherungsanlagen». Diese adressieren die IT-Sicherheit bis heute nicht detailliert. Seit 2010 fordert das BAV bei einer Typenzulassung den Nachweis eines Sicherheitsmanagementsystems, in welchem beschrieben werden muss, wie die Infrastruktur abgesichert ist. Somit war das Programm «DatacomNG» das erste, bei dem die IT-Sicherheit in diesem Masse geprüft wurde. Die nicht detaillierten Vorgaben haben zu zeitaufwendigen Diskussionen zwischen dem BAV und den beauftragten externen Gutachtern geführt. Im Rahmen

der Überarbeitung der AB-EBV wird die IT-Sicherheit ausführlich adressiert. Die Neufassung, welche voraussichtlich am 1. November 2020 in Kraft treten wird, umfasst ein Kapitel über IT-Sicherheit, welches die bisherigen Anforderungen konkretisiert. Dort wird auch eine Konformität mit den entsprechenden Standards (ISO/IEC 27001, IEC 62443) angestrebt.

Als Aufsichtsbehörde übernimmt das BAV in keinem Fall eine mitentwickelnde Rolle und auch nicht die Rolle einer unabhängigen Prüfstelle. Für diesen Prozess werden unabhängige Gutachter durch den Antragsteller beauftragt.

Beurteilung

Es sind verschiedene Vorgaben verfügbar, diese definieren aber derzeit keine detaillierten Anforderungen an die IT-Sicherheit. Diese Ausgangslage hat das Bewilligungsverfahren für die SBB AG erschwert. Die EFK begrüsst, dass das BAV mit der Anpassung der AB-EBV künftig das Thema IT-Sicherheit konkreter adressiert und entsprechende Standards zur Anwendung empfiehlt. Dadurch haben die Antragstellerin und die Gutachterin künftig konkrete Vorgaben, wie die Systeme geprüft werden.

Das sich rasch ändernde Umfeld erfordert regelmässige Anpassungen der Systemlandschaft durch die Bahnbetreiberinnen. Diese Änderungen setzen jeweils eine erneute Zulassung durch das BAV voraus, falls die Änderung aufgrund der Fehlerwahrscheinlichkeit und den Auswirkungen als PGV-pflichtig eingestuft wird. Das Bewilligungsverfahren kann je nach gewähltem Vorgehen und Systemarchitektur eine nicht unerhebliche zeitliche Verzögerung bei der Implementierung von Massnahmen verursachen. Verzögerungen können das Risiko teils erheblich vergrössern, da Schutzmassnahmen in Form von z.B. Software Patches nicht in sinnvollen Zeitrahmen umgesetzt werden können.

Empfehlung 8 (Priorität 2)

Die EFK empfiehlt dem BAV zusammen mit den Bahnen zu präzisieren, wann eine Änderung der Systemlandschaft bewilligungspflichtig ist. Weiter soll geprüft werden, inwieweit im Freigabeprozess die agilen Vorgehensweisen berücksichtigt werden können und ob die Prozesse und Verfahren optimiert werden können.

Stellungnahme des Geprüften

Die EFK empfiehlt dem BAV zusammen mit den Bahnen zu präzisieren, wann eine Änderung der Systemlandschaft bewilligungspflichtig ist. Weiter soll geprüft werden, inwieweit im Freigabeprozess die agilen Vorgehensweisen berücksichtigt werden können und ob die Prozesse und Verfahren optimiert werden können. Der Prozess Datennetze@SA, der Bestandteil der Typenzulassung des Datennetzes Datacom-NG ist, regelt sowohl die Aufschaltung sicherheitsrelevanter Anwendungen wie auch die Anpassungen am Datacom-NG selber. Dazu gehören die in der Empfehlung erwähnten «Änderungen der Systemlandschaft». Der Prozess legt die Aufgaben der SBB in diesem Zusammenhang fest. Er erlaubt eine effiziente Behandlung ohne Plangenehmigungsverfahren und ohne Einbezug des BAV. Jedoch war zum Zeitpunkt der Prüfung durch die EFK dieser Prozess noch in der Phase der Betriebserprobung und für jede Aufschaltung war eine formlose Freigabe des BAV notwendig. Nach dem Erteilen der definitiven Typenzulassung für den Prozess Datennetze@SA fallen diese Freigaben durch das BAV weg, womit die Empfehlung der EFK bei der SBB umgesetzt sein wird. Das BAV untersucht gegenwärtig mit dem Verband öffentlicher Verkehr (VöV) und direkt mit den betroffenen Bahnen, wie die Migration und der Betrieb von neuen Datennetzen bei den übrigen Bahnen in Zukunft ähnlich effizient wie bei der SBB behandelt werden kann.

Anhang 1: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967 (Stand am 1. Januar 2018), SR 614.0
Bundesgesetz über das öffentliche Beschaffungswesen (BöB) vom 16. Dezember 1994 (Stand am 1. Januar 2019), SR 172.056.1
Verordnung über das öffentliche Beschaffungswesen (VöB) vom 11. Dezember 1995 (Stand am 1. Januar 2018), SR 172.056.11
Verordnung über Bau und Betrieb der Eisenbahnen (Eisenbahnverordnung, EBV) vom 23. November 1983 (Stand am 15. Mai 2018), SR 742.141.1
Ausführungsbestimmungen zur EBV (AB-EBV) (Stand am 1. Juli 2016)

Anhang 2: Abkürzungen

AB-EBV	Ausführungsbestimmungen zur Eisenbahnverordnung
BAV	Bundesamt für Verkehr
BöB	Bundesgesetz über das öffentliche Beschaffungswesen
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
DC-NG	«Datacom-NG», Datacom Next Generation
EBV	Verordnung über Bau und Betrieb der Eisenbahnen
EFK	Eidgenössische Finanzkontrolle
ERP	Enterprise-Resource-Planning (siehe auch Glossar)
ETCS	European Train Control System (siehe auch Glossar)
FFF	Fulfillment-Factory
GE	Gigabit Ethernet (siehe auch Glossar)
GSM-R	Global System for Mobile Communications – Rail(way) (siehe auch Glossar)
I-AT	SBB Infrastruktur – Anlagen und Technologie
I-AT-TC	SBB Infrastruktur – Anlagen und Technologie – Telecom
I-AT-TC-TPP	SBB Infrastruktur – Anlagen und Technologie – Telecom – Transition Planning und Programme
IDS	Intrusion-Detection-Systeme
IEC	International Electrotechnical Commission (siehe auch Glossar)
IKT	Informations- und Kommunikationstechnik
I-NAT	SBB Infrastruktur – Netzdesign, Anlagen und Technologie
IPS	Intrusion-Prevention-Systeme
IPv6	Internetprotokoll – Netzwerkprotokoll (siehe auch Glossar)
ISO	International Organization for Standardization

ISMS	Information Security Management System (siehe auch Glossar)
IT	Informationstechnik
IT-SR	SBB Informatik – Information Security & Risk Management
KI	Kritische Infrastruktur
MPLS	Multi Protocol Label Switching (siehe auch Glossar)
NFM-P	Network-Function Manager-Paket
NMS	Network Management System
OCT	Operation Center Technik
OSS	Operation Support System
OTN	Optisches Transportnetz
QM	Qualitätsmanagement
QS	Qualitätssicherung
PSIRT	Product Security Incident Response Team
RL TZL	Richtlinie Typenzulassung für Elemente von Eisenbahnanlagen
RM	Risikomanagement
SCADA	Supervisory Control and Data Acquisition (siehe auch Glossar)
SAP	Systeme, Anwendungen und Produkte in der Datenverarbeitung – deutscher Softwarehersteller mit Sitz in Walldorf
SBB	Schweizerische Bundesbahnen
SCZ	Service Center Zutritt
SDH	Synchrone Digitale Hierarchie (Synchronous Optical Network) (siehe auch Glossar)
SIA	Schweizerischer Ingenieur- und Architektenverein (siehe auch Glossar)
SIEM	Security Information and Event Management (siehe auch Glossar)
TC	Telecom

TDM	Time-division Multiplexing (siehe auch Glossar)
USV	Unterbrechungsfreie Stromversorgung
VöB	Verordnung über das öffentliche Beschaffungswesen
VR	Verwaltungsrat

Anhang 3: Glossar

DIN ISO/IEC 27001:2013	Die internationale Norm ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements definiert Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems (ISMS).
CENELEC EN50128 CENELEC EN50129 CENELEC EN50159	Die EN 50128 ist eine europäische Norm für sicherheitsrelevante Software (Railway Control & Protection – z. B. ESTW & SA) der Eisenbahn, sowohl strecken- als auch zugseitig. Zusammen mit der EN 50129 für die Safety-related electronic systems for signaling. Die EN 50159 = Safety-related communication in transmission systems (z. B. Netz HW&SW) beschreibt die Anforderungen an die Kommunikation.
Denial of Service	Denial of Service bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Dienstes, in der Regel durch willentlich hervorgerufene Überlastung.
Enterprise-Resource-Planning	Bezeichnet die Aufgabe eines Unternehmens, Ressourcen wie Kapital, Betriebsmittel, Personal und IT-Technik rechtzeitig und bedarfsgerecht zu planen und zu steuern.
ETCS	Das European Train Control System ist ein Zugbeeinflussungssystem und grundlegender Bestandteil des zukünftigen einheitlichen europäischen Eisenbahnverkehrsleitsystems.
Gigabit Ethernet	In Computernetzwerken sind Gigabit Ethernet die verschiedenen Technologien zum Übertragen von Ethernet-Frames mit einer Geschwindigkeit von einem Gigabit pro Sekunde, wie im IEEE 802.3ab-Standard definiert.
GSM-Rail	GSM-Rail (GSM-R) ist ein digitales Mobilfunksystem, das auf dem weit verbreiteten Mobilfunkstandard GSM aufbaut, jedoch für die Verwendung bei den Eisenbahnen erweitert wurde.
HERMES	eCH-0054: HERMES Projektmanagement-Methode HERMES ist die Projektmanagement-Methode für Informatik, Dienstleistung, Service und Geschäftsorganisationen und wurde von der schweizerischen Bundesverwaltung entwickelt. Die Methode steht als offener Standard vom Verein eCH allen zur Verfügung.
IEC 62443	Die Internationale Normenreihe IEC 62443 befasst sich mit der Cybersecurity von "Industrial Automation and Control Systems (IACS)" und verfolgt dabei einen ganzheitlichen Ansatz für Betreiber, Integratoren und Hersteller.

IPv6	Internet Protocol Version 6 löst in den nächsten Jahrzehnten im Internet den IPv4-Standard ab.
ISMS	Verfahren und Vorgaben innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und kontinuierlich zu verbessern.
Layer-2-Angriffe	Sammelbegriff für unterschiedliche Angriffsmethoden auf die Funktionalitäten der OSI Layer 2.
MAC-Adresse	Die MAC-Adresse (Media-Access-Control-Adresse) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die als eindeutige Identifikation des Geräts in einem Rechnernetz dient.
MAC-Flooding	MAC-Flooding ist eine Angriffstechnik, um die Source Address Table eines Switches mit gefälschten MAC-Adressen zu fluten (Denial of Service).
MAC-Spoofing	Verändern der originalen und eindeutigen Hardwareadresse mit dem Ziel, in ein Netzwerk einzudringen, welches nur bestimmte MAC-Adressen zulässt.
MPLS	Multiprotocol Label Switching ermöglicht die verbindungsorientierte Übertragung von Datenpaketen in einem verbindungslosen Netz entlang eines zuvor aufgebauten Pfads. Dieses Vermittlungsverfahren wird überwiegend von Betreibern grosser Transportnetze eingesetzt, die Sprach- und Datendienste auf Basis von IP anbieten.
OSI-(Layer)-Modell	Das OSI-Modell (Open Systems Interconnection Model) ist ein Referenzmodell für Netzwerkprotokolle als Schichtenarchitektur. Zweck des OSI-Modells ist, Kommunikation über unterschiedlichste technische Systeme hinweg zu ermöglichen und die Weiterentwicklung zu begünstigen.
Path-Protection	End-to-End-Schutzschema, das in verbindungsorientierten Schaltkreisen in verschiedenen Netzwerkarchitekturen verwendet wird.
Port-Security	Port-Security ist ein Sicherheitsfeature von Ethernet-Switches, das es ermöglicht, jede Schnittstelle eines Switches fest mit einer MAC-Adresse (oder einer Liste von MAC- bzw. Hardware-Adressen) zu verknüpfen, sodass nur mit der erlaubten MAC-Adresse eine Kommunikation zugelassen wird.
Rollout	Vom englischen «roll out» für «ausrollen», bedeutet so viel wie Einführung.

Supervisory Control and Data Acquisition	Überwachen und Steuern technischer Prozesse mittels eines Computersystems.
SDH	SDH stellt ein synchrones Zeitmultiplex-Verfahren dar. Ziel ist die bestmögliche Ausnutzung der von Glasfasern gebotenen Übertragungskapazität.
Security Information and Event Management	Security Information and Event Management kombiniert Security Information Management und Security Event Management für die Echtzeitanalyse von Sicherheitsalarmen aus Anwendungen und Netzwerkkomponenten.
SIA-Normen	Der SIA hat mit seinem breit angewendeten und prägnanten Normenwerk anerkannte und unverzichtbare nationale Regeln der Baukunde geschaffen.
TDM-Legacy-Netz	Time-division Multiplexing ist eine Methode, bei der multiple Datenströme in einem einzelnen Signal übertragen werden. Dabei wird das Signal in viele Segmente mit sehr kurzer Dauer unterteilt. Jeder individuelle Datenstrom wird auf der empfangenden Seite anhand des Timings wieder zusammengesetzt.

Priorisierung der Empfehlungen

Die Eidg. Finanzkontrolle 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).