Deloitte.

SBB CFF FFS

Schweizerische Bundesbahnen AG

Bericht des unabhängigen Prüfers des Dienstleisters zu Kontrollen im Bereich NOVA bei der Schweizerischen Bundesbahnen AG

ISAE 3402 Typ 2

Für die Periode vom 1. Januar 2022 bis 30. September 2022

Vertraulichkeitserklärung

Dieser Bericht, einschliesslich der Beschreibung von Prüfungshandlungen und darauf bezogener Ergebnisse in Abschnitt IV, dient ausschliesslich zur Information der Schweizerischen Bundesbahnen AG (SBB) sowie der Mitglieder der Alliance SwissPass als Dienstleistungsempfänger der NOVA-Plattform während eines Teils oder des gesamten Zeitraums vom 1. Januar 2022 bis 30. September 2022, die Risiken aus Interaktionen mit dem System von SBB unterliegen sowie deren Revisoren für diesen spezifischen Auftrag, Anwendern, die Dienstleistungen für solche Unternehmen und Geschäftspartner erbringen, und Aufsichtsbehörden, die über ausreichende Kenntnisse und Kenntnisse in den folgenden Bereichen verfügen:

- Die Art der von der SBB bereitgestellten Dienste.
- Wie das System von der SBB mit assoziierten Unternehmen, Geschäftspartnern und anderen Parteien interagiert.
- Interne Kontrollen und ihre Grenzen.
- Ergänzende Benutzerentitätskontrollen («Complementary User Entity Controls») und wie sie mit den entsprechenden Kontrollen bei SBB interagieren, um die Verpflichtungen und Systemanforderungen der SBB zu erfüllen.
- Verantwortlichkeiten der Complementary User Entity Controls und wie sie sich auf die Fähigkeit der Empfänger auswirken können, die Dienste der SBB effektiv zu nutzen.
- Die Risiken, welche die Erfüllung der Serviceverpflichtungen und Systemanforderungen der SBB gefährden können, und wie Kontrollen diesen Risiken begegnen.

Dieser Bericht dient einzig dem im Bericht (Kapitel I) dargelegten Zweck und darf zu keinem anderen Zweck verwendet und keinen anderen als den oben genannten Parteien abgegeben werden.

Abkürzungsverzeichnis

AD	Active Directory
ART	Agile Release Train
ASP	Alliance SwissPass
DM	Datenmanagement
DV	Direkter Verkehr
FSS	Financial Systems & Services
IAM	Identity & Access Management
IKS	Internes Kontrollsystem
KTU	Konzessionierte Transportunternehmung
MKS DSO	Mobilitätskunden Digital Solution
NDV	Nationaler Direkten Verkehr
SAV	Service après-vente
öV	Öffentlicher Verkehr
TPS-Wechsel	Tarifperiodenstandwechsel
TU	Transportunternehmung

Inhaltsverzeichnis

Kapitel I: Bericht der unabhängigen Prüfgesellschaft über die Beschreibung der Kontrollen, deren Ausgestaltung und Wirksamkeit 03

Kapitel II: Erklärung des Dienstleisters zum internen Kontrollsystem 06

Kapitel III: Beschreibung des internen Kontrollsystems 09

Kapitel IV: Kontrollziele, dazugehörige Kontrollen und Prüfung der Wirksamkeit der Kontrollen durch Deloitte 20

Kapitel V: Sonstige Informationen durch SBB 35

Kapitel I: Bericht der unabhängigen Prüfgesellschaft über die Beschreibung der Kontrollen, deren Ausgestaltung und Wirksamkeit

Deloitte AG
Pfingstweidstrasse 11
8005 Zürich
Schweiz

Tel: +41 (0)58 279 6000
www.deloitte.ch

Kapitel I: Bericht der unabhängigen Prüfgesellschaft über die Beschreibung der Kontrollen, deren Ausgestaltungund Wirksamkeit

An das Management der Schweizerischen Bundesbahnen AG

Prüfungsumfang
Sie haben uns beauftragt, Bericht zu erstatten über die in Kapitel III beschriebenen Dienstleistungen der Schweizerischen Bundesbahnen AG (SBB) im Bereich NOVA für den Zeitraum vom 1. Januar 2022 bis zum 30. September 2022 (die «Beschreibung»). Der Bericht schliesst die Angemessenheit der Ausgestaltung und das wirksame Anwenden der Kontrollen zur Erreichung der beschriebenen Kontrollziele mit ein. Der Zweck der Beschreibung besteht darin, Dienstleistungsbezügern Informationen über die NOVA-Dienstleistungen der SBB zu vermitteln, insbesondere über die Kontrollen, die vorgesehen sind, um die von der SBB definierten Kontrollziele zu erfüllen.

Verantwortung des Dienstleistungserbringers
Die Schweizerische Bundesbahnen AG ist verantwortlich für:

- das Erstellen der Beschreibung sowie der Erklärung in Kapitel II hinsichtlich der Vollständigkeit und Angemessenheit der Darstellung als Ganzes, sowie der darin enthaltenen Aussagen;
- das Erbringen der in der Beschreibung erwähnten Dienstleistungen;
- das Festlegen der Kontrollziele;
- die Identifikation der Kriterien und die Ausgestaltung und Implementierung sowie die wirksame Anwendung der Kontrollen zur Erreichung der beschriebenen Kontrollziele.

Unabhängigkeit und Qualitätskontrolle
Bei der Durchführung des Auftrags haben wir ausserdem die Vorschriften zur Unabhängigkeit und Ethik des Code of Ethics for Professional Accountants, publiziert vom International Ethics Standards Board for Accountants, eingehalten. Dieser Code basiert auf den Prinzipien der Integrität, Objektivität, professionellen Kompetenz und Verhalten, Vertraulichkeit sowie der Sorgfaltspflicht.

Deloitte setzt den International Standard on Quality Control 1 um und unterhält entsprechend ein umfassendes System zur Qualitätskontrolle einschliesslich schriftlicher Leitlinien und Prozesse bezüglich der Compliance über ethische Ansprüche, berufliche Verhaltensanforderungen und den anwendbaren rechtlichen und regulatorischen Vorschriften.

Verantwortung des Prüfers des Dienstleistungserbringers
Unsere Verantwortung besteht darin, aufgrund unserer Prüfungshandlungen ein Prüfungsurteil zur Beschreibung der SBB und der Ausgestaltung und Wirksamkeit der in der Beschreibung enthaltenen Kontrollen und der damit verbundenen Kontrollziele zu machen. Wir haben unsere Prüfung in Übereinstimmung mit dem International Standard on Assurance Engagements (ISAE) 3402 «Assurance reports on controls at a service organization», herausgegeben vom International Auditing and Assurance Standards Boards (IAASB), durchgeführt. Dieser Standard verlangt die ethischen Grundsätze unseres Berufsstandes einzuhalten und die Prüfung so zu planen und durchzuführen, um mit hinreichender Sicherheit ein Prüfungsurteil abgegeben zu können, dass die Beschreibung der Systeme und Kontrollen im Zusammenhang mit den Tätigkeiten als Dienstleistungserbringer in allen wesentlichen Belangen sachgerecht dargestellt ist und die Kontrollen angemessen ausgestaltet und wirksam waren für den Zeitraum vom 1. Januar 2022 bis zum 30. September 2022.

Die Prüfung der Beschreibung des Systems und der Angemessenheit der Ausgestaltung und Wirksamkeit der Kontrollen eines Dienstleistungserbringers beinhaltet die Durchführung von Prüfungshandlungen zum Erhalt von Prüfungsnachweisen hinsichtlich Beschreibung und Angemessenheit der Ausgestaltung und Wirksamkeit der Kontrollen. Die durchgeführten Prüfungshandlungen liegen im Ermessen des Prüfers. Sie schliessen die Risikobeurteilung ein, ob die Beschreibung des Systems des Dienstleistungserbringers nicht sachgerecht, und ob die Kontrollen nicht ausreichend ausgestaltet oder wirksam waren. Unsere Prüfungshandlungen schlossen diejenigen Funktionsprüfungen zur Wirksamkeit dieser Kontrollen ein, die wir als notwendig erachteten, um mit angemessener Sicherheit ein Prüfungsurteil darüber abzugeben, dass die in der Beschreibung erläuterten Kontrollziele erreicht wurden. Ein solcher Prüfungsauftrag umfasst auch eine Beurteilung der Beschreibung als Ganzes, der Angemessenheit der beschriebenen Kontrollziele sowie der Eignung der durch die SBB in Kapitel II dargestellten Kriterien.

Wir sind der Auffassung, dass die von uns erlangten Prüfungsnachweise eine ausreichende und angemessene Grundlage für unser Prüfungsurteil bilden.

Inhärente Beschränkungen der Kontrollen des Dienstleistungserbringers
Die Beschreibung der SBB wurde mit dem Ziel verfasst, den allgemeinen Bedürfnissen der Mitglieder der Alliance SwissPass und deren Abschlussprüfern zu entsprechen. Deshalb konnten nicht alle Aspekte des Systems berücksichtigt werden, die Kunden in ihrem eigenen Umfeld als wichtig erachten würden. Kontrollen bei einem Dienstleistungserbringer können zudem naturgemäss nicht sämtliche Fehler oder Unterlassungen im Bereich der IT-Dienstleistungen verhindern oder aufdecken. Die Übertragung jeglicher Prüfungsresultate über die korrekte Darstellung der Beschreibung oder Prüfungsaussagen über die Angemessenheit der Ausgestaltung oder Wirksamkeit der Kontrollen und mit ihnen zusammenhängenden Kontrollzielen in die Zukunft birgt das Risiko, dass die Kontrollen bei einem Dienstleistungserbringer nicht mehr angemessen oder nicht mehr wirksam sind.

Prüfungsurteil
Unser Prüfurteil wurde auf der Grundlage der in diesem Bericht dargelegten Informationen gebildet. Die Kriterien, die wir bei der Bildung unseres Prüfurteils verwendet haben, sind die in der Erklärung der SBB beschriebenen (Kapitel II). Nach unserer Beurteilung des im vorstehenden Abschnitt dargelegten Sachverhaltes trifft in allen wesentlichen Belangen insgesamt Folgendes zu:

a. Nach unserer Beurteilung und basierend auf den in der Erklärung des SBB (vgl. Kapitel II) genannten Kriterien und Kontrollziele, gibt die Beschreibung - mit Ausnahme der im vorstehenden Abschnitt dargelegten Beschränkung - die Ausgestaltung und Implementierung der Kontrollkreise ihrer Organisation für den Zeitraum 1. Januar 2022 bis zum 30. September 2022 sachgerecht wieder.

b. Sofern die beschriebenen Kontrollen im Zeitraum vom 1. Januar 2022 bis zum 30. September 2022 wirksam gewesen waren und die Dienstleistungsbezüger ihre jeweiligen ergänzenden Kontrollen, welche bei der Konzeption der Kontrollen von SBB berücksichtigt wurden, im gleichen Zeitraum wirksam durchführten, kann mit einer angemessenen Sicherheit davon ausgegangen werden, dass die Ausgestaltung der Kontrollen zur Erreichung der jeweiligen Kontrollziele geeignet war.

c. Die geprüften Kontrollen waren im Zeitraum vom 1. Januar 2022 bis zum 30. September 2022 wirksam. Die geprüften Kontrollen entsprachen denjenigen Kontrollen, die zur Erreichung der in der Beschreibung enthaltenen Kontrollziele, auf der Basis einer angemessenen Sicherheit, notwendig waren.

Hervorhebung eines Sachverhaltes
Die SBB gibt in ihrer Beschreibung an, dass sie über Kontrollen verfügt, welche das Kontrollziel «Zugriffsicherheit NOVA Abrechnung», gewährleisten bzw. unterstützen. Wie in Kapitel IV des Berichts erwähnt, wurden durchzuführende Kontrollen während der Berichtsperiode vom 1. Januar 2022 bis 30. September 2022 nicht durchgeführt, da die Durchführung nicht im Berichtszeitraum fällig war. Die betroffene Kontrolle wird typischerweise im Oktober durchgeführt.

Daher konnten wir die folgende Kontrolle im Zusammenhang mit Kontrollziel 2 nicht auf deren Wirksamkeit prüfen:
Kontrollziel 2 – Die Kontrollen stellen angemessen sicher, dass der Zugang zu NOVA Abrechnung genehmigt wird und auf der Grundlage der Arbeitsfunktionen angemessen ist; Zugriffsrechte von gekündigten/ausgetretenen Benutzern zeitnah angepasst wird sowie die hochprivilegierten Accounts angemessen vergeben sind

- **Kontrolle 2.3:** Überprüfung der Benutzerzugriffsrechte

Beschreibung der Prüfungshandlungen
Die geprüften Kontrollen sowie Art, Zeitpunkt und Ergebnis der Prüfungen sind in Kapitel IV aufgeführt.

Vorgesehene Nutzung und Verwendung
Da wir von der SBB beauftragt wurden, sind dieser Bericht und die Prüfungsergebnisse in Kapitel IV zur Verwendung durch die SBB bestimmt.

Wir stimmen einer Weitergabe dieses Berichts durch die SBB an die Mitglieder der Alliance SwissPass, die ihre Dienstleistungen im Bereich NOVA während einem Teil oder dem gesamten Zeitraum von 1. Januar 2022 bis zum 30. September 2022 in Anspruch genommen haben,und deren Abschlussprüfer ausschliesslich im Ganzen zu. Wir gehen davon aus, dass die Kunden und Abschlussprüfer unseren Bericht neben weiteren Informationen über die von den Kunden selbst zu verantwortenden Kontrollen für ihre Beurteilung der Risiken wesentlicher falscher Darstellungen der Abschlüsse der Kunden angemessen zu würdigen wissen. Wir übernehmen keine Verantwortung oder Haftung gegenüber den Kunden oder deren Abschlussprüfern.

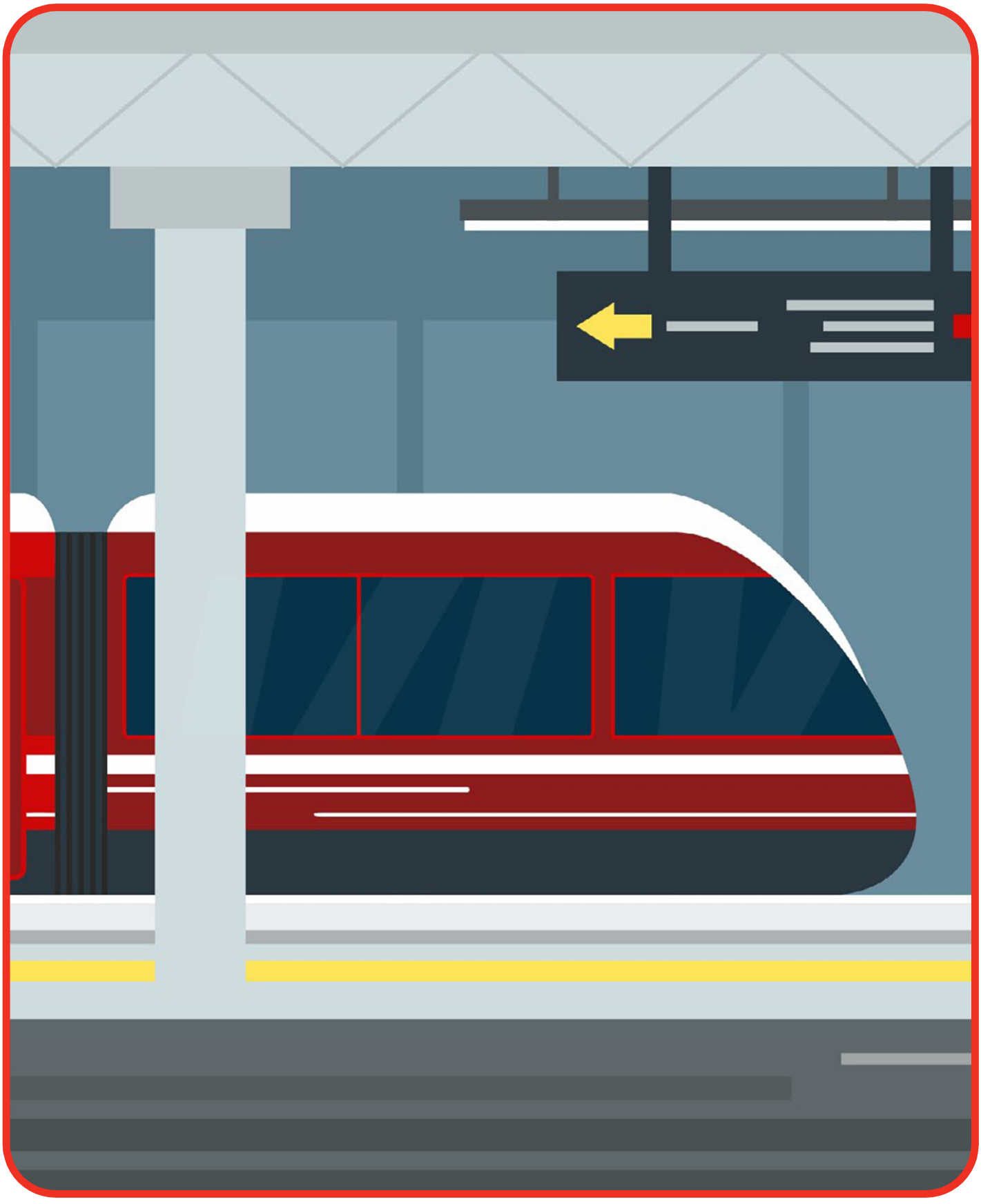
Deloitte AG

Fabien Lussu
Partner

Simon Brander
Director

Zürich, 12. Dezember 2022

Kapitel II: Erklärung des Dienstleisters zum internen Kontrollsystem



Kapitel II: Erklärung des Dienstleisters zum internen Kontrollsystem

Schweizerische Bundesbahnen AG
Hilfikerstrasse 1
3000 Bern 65

An das Management der
Deloitte AG
Pfingstweidstrasse 11
8005 Zurich

Erklärung des Dienstleisters zum internen Kontrollsystem
Die Schweizerische Bundesbahnen AG (SBB) hat die beigefügte Beschreibung des Systems der IT-Dienstleistungen von SBB bezüglich der Leistungen (Kapitel III «Beschreibung der IT-Dienstleistungserbringung der SBB») für den Zeitraum vom 1. Januar 2022 bis zum 30. September 2022 auf Grundlage der in den nachfolgenden Abschnitten aufgeführten Kriterien erstellt. Diese enthält auch eine Beschreibung der von den Dienstleistungsempfängern selbst durchzuführenden Kontrollen. Wir gehen davon aus, dass unsere Dienstleistungsempfänger (d.h die Mitglieder der Alliance SwissPass) und deren Prüfer die Informationen über die von den Dienstleistungsempfängern selbst durchgeführten Kontrollen im Rahmen der Beurteilung der Einhaltung Risiken wesentlicher falscher Angaben der Jahresrechnung der Dienstleistungsempfänger verstehen. Die in Kapitel IV dargestellten spezifischen Kontrollziele und Kontrollen sind integraler Bestandteil der Beschreibung.

Der Zweck der Beschreibung besteht darin, den Dienstleistungsbezügern Informationen über das Kontrollsystem der IT-Dienstleistungen der SBB zu vermitteln, insbesondere über die Kontrollen, die vorgesehen sind, um die von SBB definierten Kontrollziele im Zusammenhang mit der Entwicklung, der Wartung und dem Betrieb von NOVA zu erfüllen.

Beschreibungskriterien
Wir bestätigen nach bestem Wissen, dass:

1) die beiliegende Beschreibung des Kontrollsystems der NOVA-Umgebung («System») des Dienstleistungsempfängers in der Berichtsperiode vom 1. Januar 2022 bis zum 30. September 2022 zutreffend darstellt. Grundlage dieser Erklärung ist der Umstand, dass die Beschreibung

   a. die Ausgestaltung und Implementierung des Systems wiedergeben. Dies berücksichtigt

      i. die Art der Dienstleistungen, gegebenenfalls einschliesslich der Art der verarbeiteten Geschäftsvorfälle;

      ii. den Prozess für die Berichterstattung an die Dienstleistungsempfänger;

      iii. gegebenenfalls von einer Subservice-Organisation erbrachte Dienstleistungen, einschliesslich der Frage, ob die «carve-out» Methode oder die inkludierende Methode in Bezug auf sie verwendet wurde;

      iv. Kontrollen, bei denen wir im Rahmen der Ausgestaltung des Systems davon ausgegangen sind, dass sie von den Dienstleistungsempfängern implementiert würden. Diese Kontrollen werden, neben den entsprechenden Kontrollzielen, in der Beschreibung mit angegeben, sofern dies zur Erreichung der Kontrollziele notwendig ist;

      v. weitere Aspekte unseres Kontrollumfeldes, unseres Risikobewertungsprozesses, unseres Informationssystems (einschliesslich der damit verbundenen Geschäftsprozesse) und unserer Kommunikations-, Kontroll- und Überwachungstätigkeiten, die für die Durchführung und Berichterstattung von Geschäftsvorfällen der Dienstleistungsempfänger relevant waren;

   b. die relevanten Informationen über Änderungen unseres Systems im Zeitraum vom 1. Januar 2022 bis zum 30. September 2022 enthält; und

   c. keine relevanten Informationen über das beschriebene System verfälscht oder vermissen lässt. Hierbei ist zu berücksichtigen, dass die Beschreibung der Prozesse darauf ausgelegt ist, die Informationsbedürfnisse einer Vielzahl von Dienstleistungsempfängern und deren Prüfern zu erfüllen. Sie kann daher zwangsläufig nicht jeden Aspekt darstellen, den ein Dienstleistungsempfänger mit Blick auf sein eigenes Betriebsumfeld für wichtig erachtet;

2) die Kontrollen zur Erreichung der dargestellten Kontrollziele angemessen ausgestaltet und in dem der Prüfung zugrundeliegenden Zeitraum vom 1. Januar 2022 bis zum 30. September 2022 wirksam waren. Grundlage dieser Einschätzung ist die Tatsache, dass

   a. die Risiken, die die Erreichung der beschriebenen Kontrollziele beeinträchtigen können, von der SBB identifiziert wurden;

   b. die beschriebenen Kontrollen, vorausgesetzt sie werden beschreibungskonform durchgeführt und die Dienstleistungsbezüger ihre jeweiligen ergänzenden Kontrollen, welche bei der Konzeption der Kontrollen von SBB berücksichtigt wurden, im gleichen Zeitraum wirksam durchführten, eine angemessene Sicherheit bieten, dass diese Risiken die Erreichung der beschriebenen Kontrollziele nicht beeinträchtigen; und dass

   c. die Kontrollen im Zeitraum vom 1. Januar 2022 bis zum 30. September 2022 beschreibungskonform durchgeführt wurden. Dies beinhaltet, dass die manuellen Kontrollen nur durch solche Mitarbeitenden durchgeführt wurden, die dazu befähigt und berechtigt sind.

Schweizerische Bundesbahnen SBB,

IT-SCP-PLB-CPT1
Bern, 12.12.2022

QES Qualifizierte elektronische Signatur · EU-Recht
Signiert auf Skribble.com

Michael Klötzli
Mandatsträger IT/Services

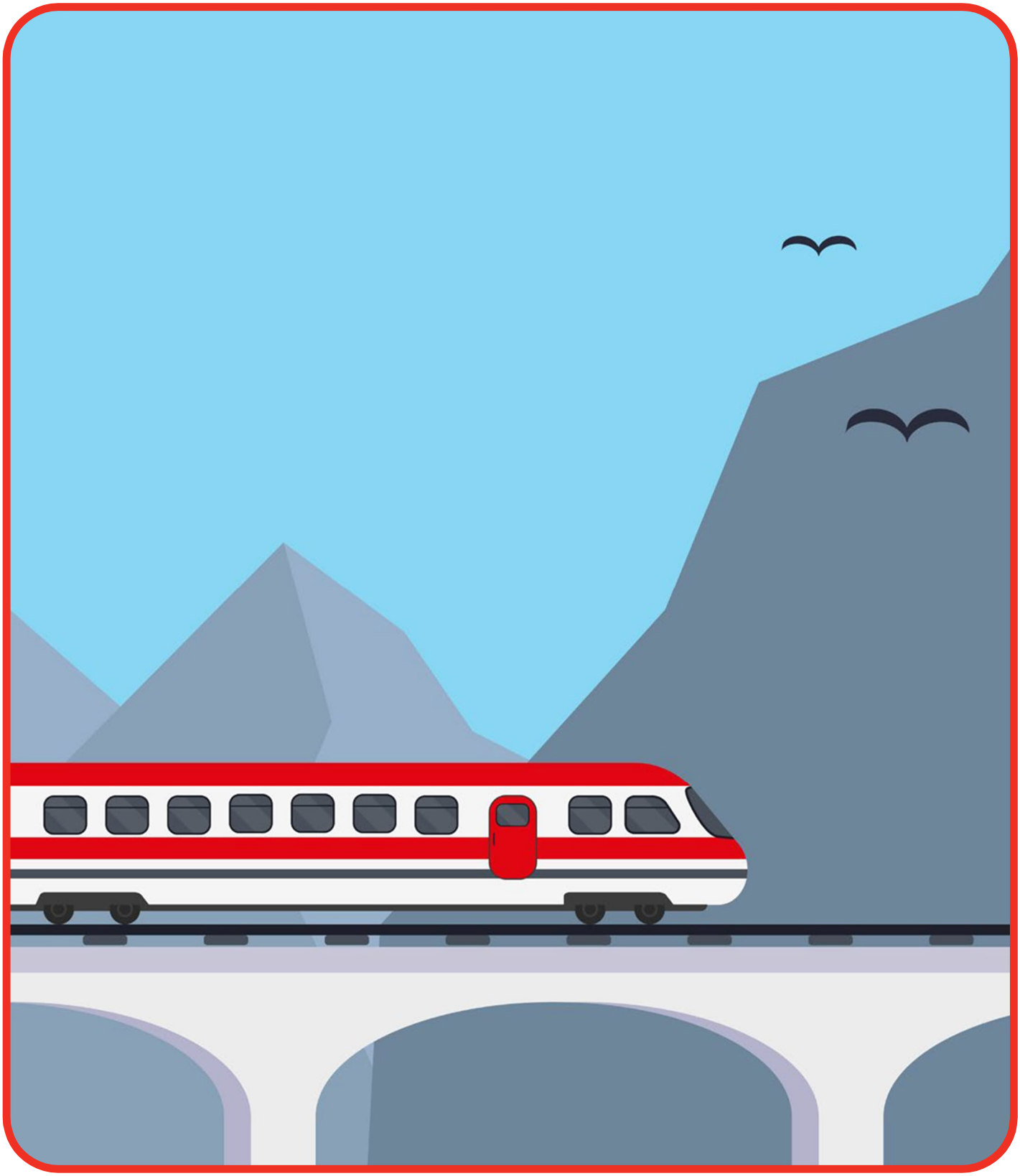
Monika Kaiser Zengaffinen
Leiterin IT Customer Journey, SBB AG
12.12.2022

QES Qualifizierte elektronische Signatur · EU-Recht
Signiert auf Skribble.com

Monika Kaiser Zengaffinen
Mitglied der Geschäftsleitung IT
Leiterin IT-Customer Journey

Bern, 12. Dezember 2022

Kapitel III: Beschreibung des internen Kontrollsystems



Kapitel III: Beschreibung des internen Kontrollsystems

3.1. Zielsetzung des Berichts

Die Transportunternehmen (TU) führen in der Regel regelmässig Revisionen ihrer Verkäufe und Vertriebskanäle durch. Als zentrale Verkaufsplattform spielt NOVA dabei eine wichtige Rolle. In diesem Rahmen oder unabhängig davon besteht das Bedürfnis, jeweils im Rahmen des Jahresabschlusses einen Prüfbericht zur NOVA-Plattform zu erhalten.

Der Bericht deckt die betrieblichen Aktivitäten ab, die innerhalb von NOVA einen Einfluss auf die finanzielle Berichterstattung haben können. Dazu gehören das Berechtigungsmanagement, das Changemanagement und die Prozesse zur Änderung der finanzrelevanten Stammdaten. Die korrekte Datenübertragung zwischen NOVA Anbieter und NOVA Abrechnung sowie die Wiederherstellung der Daten in NOVA Abrechnung gehören ebenfalls dazu.
Die Prozesse in Bezug auf die korrekte Datenzulieferung der Vermittler (insbesondere die Berechnung von Verteilschlüsseln) oder den Datenschutz über die NOVA-Plattform sind nicht Teil dieses Berichts.

Die Adressaten dieses Berichts sind die Alliance SwissPass und ihre Mitglieder.

3.2. Betrieb von NOVA durch die SBB

Die SBB hat im Rahmen des Mandats im Direkten Verkehr die NOVA-Plattform mit Erhalt des Mandats 2012 beginnend erstellt und betreibt diese heute im Auftrag der Alliance SwissPass, deren Mitglieder die Eigner der Plattform sind.

Die SBB ist für die Operationen verantwortlich, die von der Ein- und Ausgabeschnittstellen von NOVA Anfrage bis zu NOVA Abrechnung durchgeführt werden. Jedes Transportunternehmen, das einen mit NOVA verbundenen Kanal hat, ist selbst für die bei ihm durchgeführten Operationen verantwortlich.

NOVA Anbieter sowie die darunterliegende Infrastruktur (Datenbank und Betriebssystem) werden bei dem externen Provider «T-Systems» gehostet sowie Backups erstellt, welcher auch für den laufenden Betrieb der entsprechenden Infrastruktur verantwortlich ist. Dasselbe gilt für die SAP-Plattform, auf der NOVA Abrechnung basiert.

Der ISAE3402 Type 2 Report von T-Systems beschreibt die IT Basis Infrastruktur Services, welche von den Data Center Zollikofen und Bern bereitgestellt werden und schliesst den Bericht eines unabhängigen Prüfers, die durchgeführten Tests und deren Ergebnisse ein. Folgende Inhalte deckt der Bericht ab:

- Beschreibung der Infrastruktur-Services
- Beschreibung des Kontrollumfelds, der Informationskommunikation, der Überwachung und der Risikobewertungsprozesse
- Führung und Aufsicht
- Beschreibung der IT General Controls
- Kontrollziele und Kontrollen
- Complementary User Entity Controls
- Durchgeführte Kontrollen, Tests und Testresultate
- Massnahmenplan

3.3. Aufbau und Komponenten von NOVA

Die NOVA-Plattform ist das zentrale Vertriebs-Backend des öffentlichen Verkehrs Schweiz, über welches die angeschlossenen Transportunternehmen Angebote erstellen und über unterschiedliche Vertriebskanäle verkaufen können. Die NOVA-Plattform stellt neben dem Sortiment von DV- und Verbundfahrausweisen auch die nötigen Funktionen im Zusammenhang mit dem SwissPass, Personalisierung, E-Tickets und Service-Après-Vente zur Verfügung, so dass die Reisenden einen nahtlosen öV erleben können.

Die NOVA-Plattform besteht aus zahlreichen Komponenten, die neben dem Vertrieb von öV-Leistungen auch wichtige Funktionen in anderen Prozessen wie der Kontrolle von Billetten oder der Verwaltung von Kundendaten, Ausweisen und Verträgen einnehmen. Bei dem relevanten Geschäftsprozess «Verkauf und Erstattung von öV-Leistungen» sind die beiden Komponenten NOVA Anbieter und NOVA Abrechnung involviert. Die anderen NOVA Komponenten spielen keine Rolle bei diesem Geschäftsprozess und werden im Rahmen von diesem Bericht nicht weiter berücksichtigt.

Die Vertriebskanäle sind die Distributionswege, worüber Artikeln und Angebote verkauft werden. Ein Vertriebskanal kann entweder bedient (Schalteranwendung, Chauffeurgeräte) oder unbedient (Automaten, Webshops, Mobile Applikationen) sein. Nur Transportunternehmen (z.B. SBB, ZVV, BLS, TPG, RBS) oder Verbunde (z.B. Mobilis, Ostwind, A-Welle) und deren Partner dürfen gemäss den NOVA Nutzungsbedingungen aktuell Leistungen verkaufen. Die Vertriebskanäle liegen in der Verantwortung der Transportunternehmen und Verbunde. Entsprechend sind diese nicht Bestandteil dieses Berichts.

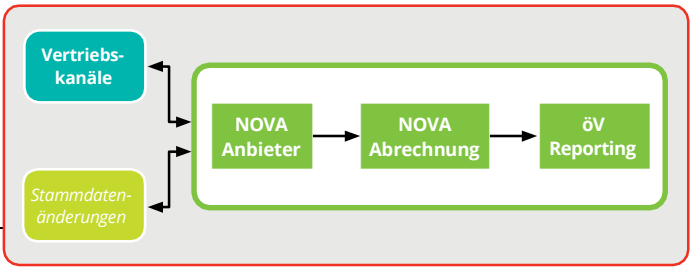
NOVA Anbieter ist die Komponente der NOVA-Plattform, welche sicherstellt, dass allen Verkäufern von öV-Leistungen (Leistungsvermittler) nach einheitlichen Kriterien erstellte und tarifierte Angebote des öffentlichen Verkehrs (öV) der Schweiz zur Verfügung stehen. Konkret übernimmt NOVA Anbieter die gesamte Preisberechnung für öV-Billette sowie die Anteilszuordnung pro KTU gemäss Leistungserbringung. Zudem verwaltet NOVA Anbieter die gesamte Verkaufsabwicklung und -prozessierung, welche gewährleistet, dass an Vertriebssystemen erfolgte Transaktionen für öV-Leistungen korrekt erfasst und alle relevanten Informationen für die Ertragsverteilung in die zentralen Finanz- und Reportingsysteme (NOVA Abrechnung) der öV-Branche einfliessen.

NOVA Abrechnung (auch «öV-Abrechnung») ist eine Kombination von SAP-Modulen, welche die Leistungsdaten von NOVA Anbieter entgegennimmt und für die weiteren Finanz- und Reportingsysteme der öV-Branche aufbereitet.

Täglich wird im Hintergrund automatisiert ein Verdichtungsprogramm gestartet, welches die Leistungen auf Duplikate prüft. Bei erfolgreicher Prüfung werden die Leistungen in die endgültige Statistik- und Finanztabelle geschrieben. Die Daten in der Finanztabelle sind verdichtet (Optimierung der Datenstruktur) und bilden die Grundlage für den Monatsabrechnung.

Bevor die Monatsabrechnung für den öV-Schweiz durchgeführt wird, müssen verschiedene Stammdaten (TU als Geschäftspartner pflegen, TU einer Abrechnungsstelle zuweisen, Daten für den PORin-Ticket Parallelbetrieb erstellen) gepflegt werden. Im Periodenabschluss wird entschieden, welche Leistungsdaten im Abrechnungslauf verarbeitet werden. Nach dem Runden und Ausgleichen werden aus der Finanztabelle «Billable Items» (abrechenbare Positionen, kurz BITs) erzeugt. Diese werden anschliessend in einem Abrechnungs- und Fakturierungslauf verarbeitet und die Daten stehen für das öV-Reporting zur Verfügung. Während der Parallellaufzeit von Backoffice und NOVA Abrechnung wird das Reportingsystem PORin-Ticket mit verschiedenen Files zusätzlich beliefert.

ÖV-Reporting als web-basierte SAP Fiori Applikation ist ein Bestandteil von NOVA Abrechnung, auf welcher registrierte Benutzer Abrechnungs- und Verkaufsinformationen ihres Unternehmens strukturiert abrufen können. Auswertbar sind alle Leistungen, welche über die NOVA-Plattform verkauft werden. Für die Auswertung-Reports werden SAP Fiori Analytical List Pages verwendet. Die Datenquellen für die Berichte im öV-Reporting sind die Tabellen in SAP, welche von NOVA Abrechnung verwendet werden. Diese Tabellen werden jede Nacht (Statistik / Marketing) oder einmal im Monat (Finanzen) inklusive Stammdaten aufbereitet. Diese Tabellen werden mit Streamworks befüllt.
Streamworks ist ein IT-Tool, in welchem Prozessautomatisierungen hinterlegt werden können sowie überwacht werden von einem spezialisierten Team. Abbrüche werden überwacht, Fehler korrigiert und Übertragungen neu gestartet. Die Überwachung ist in das interne Kontrollsystem der NOVA Abrechnung integriert und das Ergebnis der Überwachung wird monatlich rapportiert. Streamworks bietet seit Jahrzehnten bei den SBB eine zentrale Sicht über verschiedenste Technologien, Applikationen und deren Schnittstellen hinweg. Als zentraler Scheduler orchestriert die Plattform das Zusammenspiel auch in der NOVA-Plattform.
Mit Streamworks automatisierte regelmässig wiederkehrende Prozesse werden sauber abgearbeitet und zentral überwacht und im Störungsfall wird aktiv die Supportorganisation aufgeboten.



3.4. Abgrenzung innerhalb der Systemlandschaft

Ausklammerung der Prisma-Plattform

Seit den ersten Verkäufen von NOVA 2016 werden die beiden Verkaufsplattformen NOVA und Prisma parallel betrieben. Dabei wird laufend das bestehende Sortiment von Prisma nach NOVA migriert. Die TU haben Stand 2022 ihre Vertriebskanäle weitgehend auf NOVA migriert; für Restsortimente, die nicht oder nicht mehr in bisheriger Form auf NOVA verfügbar sind, wird Prisma noch weiterverwendet. Prisma wird auch als Fallback bei einem Unterbruch von NOVA genutzt. Mittlerweile werden rund 90% der Umsätze im öV Schweiz über NOVA erzielt.

Wesentliche Artikel auf Prisma sind FVP (Fahrvergünstigung Personal der Transportunternehmen; Pauschalfahrausweis), Abrechnung Militär (Marschbefehl; Pauschalfahrausweis) sowie Drittgeschäftsprodukte; welche zusammen rund 6% des Gesamtumsatzes im öV-Schweiz ausmachen. Noch über Prisma abgewickelte Verkäufe von regulären Fahrausweisen, die auch auf NOVA verfügbar wären, machen ca 4% des Gesamtumsatzes aus (Auswertung 1. Halbjahr 2022).

Prisma wird seit einiger Zeit nicht mehr weiterentwickelt. Seit 2021 werden auch keine neuen Artikel mehr eröffnet (das war bis 2020 als Fallback noch der Fall) und die bestehenden Artikel werden laufend terminiert (d.h. Vergabe eines finalen letzten Verkaufstages).
Die Ablösung der Altsysteme ist ein wichtiger Meilenstein in der Weiterentwicklung der Vertriebssysteme der öV-Branche. Es ist geplant, per Fahrplanwechsel im Dezember 2023 den Verkauf über die Prisma-Plattform einzustellen (fester Bestandteil der Mehrjahresplanung der Alliance SwissPass).

Die Prisma-Plattform befindet sich – im Gegensatz zur NOVA Plattform – im Eigentum der SBB und nicht der Alliance SwissPass. Der Umfang des vorliegenden Berichts wird daher unter Berücksichtigung der Eigentumsverhältnisse auf die NOVA Plattform beschränkt und die Prisma-Plattform bewusst ausgeklammert.

Ausklammerung weiterer Vertriebsplattformen und Vertriebssysteme (Insellösungen)

Ebenso sind weitere TU- oder verbundeigene Vertriebssysteme ausgeklammert, die ausserhalb der NOVA Plattform ihre Verkäufe realisieren bzw. Einnahmen verteilen. Diese decken nur die TU-internen Bedürfnisse ab (z.B. das Verkaufssystem für eine Bergbahn). Diese Systeme sind weder im Eigentum der Alliance SwissPass noch liegen sie in der Betriebsverantwortung der SBB.

Ausklammerung PORin-Ticket[1]

PORin-Ticket war lange Zeit die gemeinsame Plattform für Reporting und Auswertungen der öV-Branche für die getätigten Verkäufe. Primäre Quelle für PORin-Ticket waren die Verkäufe über Prisma. Mit dem Aufbau der NOVA Plattform wurde 2015 entschieden, auch den Reportingteil direkt in NOVA zu integrieren. Dafür wurde auf Basis von SAP Brim (MP3) das öV-Reporting aufgebaut.

[1] PORin ist der Name des Lieferanten

Bis Ende 2022 weisen PORin-Ticket und öV-Abrechnung die gleichen Verkaufszahlen aus (Datenlieferung NOVA an PORin-Ticket und Prisma an NOVA). Ab 2023 wird PORin-Ticket nicht mehr beliefert und steht nur noch als «read-only» für historische Daten zur Verfügung.

Auf PORin-Ticket wurden in der Vergangenheit die Berechnung zur Abgrenzung von Fahrausweisen mit einer Gültigkeit über den Monatswechsel hinaus durchgeführt (z.B. bei einem Halbtax mit einer Gültigkeitvon einem Jahr wird der Ertrag über die gesamte Gültigkeitsperiode verteilt). Während PORin-Ticket dies auf Basis des Verkaufsdatums berechnete, ist NOVA Abrechnung in der Lage, dies auf Basisdes ersten Gültigkeitstages zu berechnen. Da letztere Methode aus Sicht des Konsums genauer ist, wurde per 1. Januar 2022 im Nationalen Direkten Verkehr (NDV)[2] verbindlich branchenweit auf die Abgrenzungsberechnung gemäss NOVA Abrechnung umgestellt. Die Tarifverbünde, welche monatsübergreifendeFahrausweise bisher individuell und ausserhalb von PORin-Ticket in ihren eigenen Systemen gelöst haben, werden per 1. Januar 2024 ebenfalls auf die Berechnungslogik nach Gültigkeitstag auf NOVA Abrechnung umstellen[3].

3.5. Schnittstelle zwischen NOVA Anbieter-und NOVA Abrechnung

Die Leistungsdaten (Tickets oder Abonnements) aus NOVA Anbieter werden kontinuierlich an NOVA Abrechnung übertragen. NOVA Abrechnung meldet den Status der Leistungen an NOVA Anbieter zurück. Die Übertragung aller Leistungen wird täglich und automatisch geprüft. Sollte eine Leistung nicht übertragen werden, wird dieser Fehler täglich wieder rapportiert, bis die Leistung korrekt übertragen wurde.

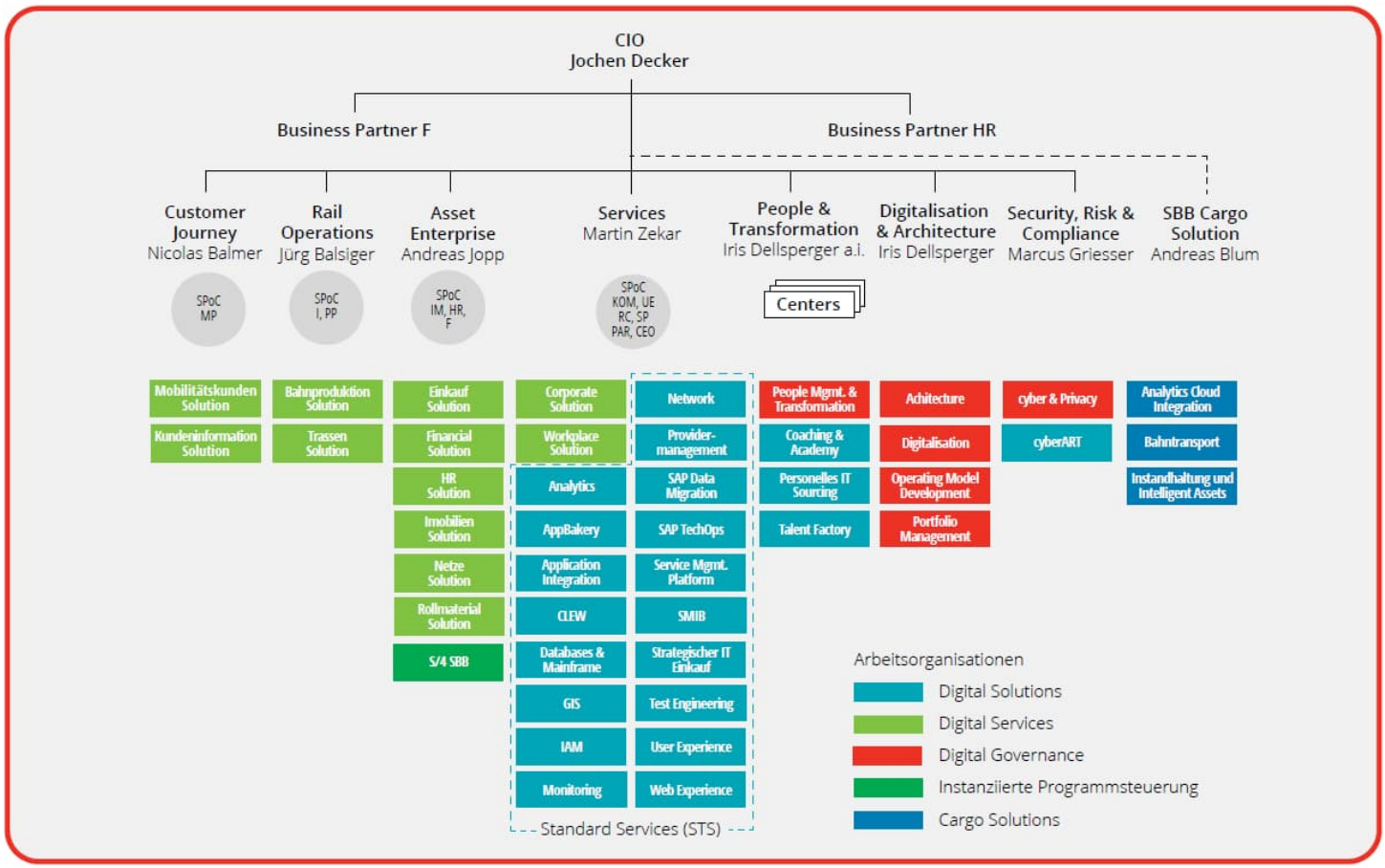
NOVA Anbieter beliefert NOVA Abrechnung mit Daten über zwei Schnittstellen: «LeistungNotification» und «INTRA-Datenrelease». Leistungen (Tickets) werden in der LeistungNotification an NOVA Abrechnung geschickt. Der INTRA-Datenrelease beinhaltet verschiedene für die NOVA Abrechnung relevante Stammdaten. Jede verarbeitete Nachricht wird mit einer Rückantwort (erfolgreich/ fehlerhaft) bei NOVA Anbieter quittiert. Die erfolgreich verarbeiteten Leistungen werden mit den vorhandenen Stammdaten angereichert und in der temporären Statistiktabelle zwischengespeichert, wo sie für die Weiterverarbeitung innerhalb des Abrechnungsprozesses bereitgestellt werden. Die Leistungen werden von NOVA Anbieter alle 30 Minuten gesendet. Leistungen mit der Rückantwort «fehlerhaft» werden einmal täglich neu gesendet.

[2] Die Schweiz besitzt drei verschiedene Tarifsysteme: der NDV (Nationale Direkte Verkehr) ist streckenbasierter Tarif innerhalb der Schweiz, welcher schweizweit geregelt ist; er wird teilweise überlagert durch die 18 Tarifverbunde, welche einen regionalen, zonenbasierten Tarif anbieten. Als letzte Kategorie gilt der «Interne Verkehr»; darunter fallen Tarife, die nur ein TU betreffen und somit keine übergreifende Koordination erfordern (z.B. eine Bergbahn).

[3] Entscheid in der Kommission Vertrieb vom 29.08.2022

3.6. Organisation und Verantwortlichkeiten

Die SBB Informatik besteht aus Digital Solutions, darunter MKS (Mobilitätskunden), und Digital Services (Stand: 31.7.2022).



Die Mission von MKS ist die Implementierung der digitalen Vorgaben der Leistungsbesteller zu Angebot, Sortiment, Preise, Vermarktung, Kundeninformation, Services, Vertriebskanäle und Kundenbegleitung und die Sicherstellung deren digitale Operationalisierung gegenüber Mobilitätskunden und internen Anwendern. MKS wird von Roger Bula (Solution Manager), Santiago Garcia (Solution Train Engineer) und Harald Alferi (Solution Architect) geleitet. Zu MKS gehören der NOVA Agile Release Train (NOVA ART) sowie der Financial Systems & Services Agile Release Train (FSS ART).

Der NOVA ART ist für NOVA Anbieter zuständig und setzt sich aus 14 Teams zusammen, während die 4 Teams vom FSS ART unter anderem für NOVA Abrechnung zuständig sind. Die Benutzerverwaltung in NOVA Anbieter liegt in der Verantwortung des NOVA Partnermanagement Teams. Weitere Teams sind für Detailaspekte verantwortlich, wie beispielsweise das IAM Team für den SwissPass Login.

Das Team «öV-Governance» ist für die Abnahme der Artikel auf NOVA sowie für die Abnahme an einem Vertriebskanal zuständig. Jedes neue Produkt, welches auf NOVA angeboten wird, muss gemäss den Regeln und Kriterien von «öV-Governance» abgenommen werden, bevor es verkauft werden kann. Dasselbe gilt für jeden neuen Vertriebskanal, über welchen die öV-Produkte verkauft werden.

Betriebliche Prozesse im NOVA Anbieter

3.7. Berechtigungsmanagement

Es existieren diverse Zugriffsrechte für NOVA Komponenten oder unterstützende Infrastruktur, die im Rahmen des täglichen Betriebs-Funktionstrennungen in den Prozessen sicherstellen. Die Trennung kritischer Funktionen wird überprüft, um Konflikte zu vermeiden. Nichtdestotrotz hat speziell die kontinuierliche Gewährleistung des 4-Augenprinzips bei wesentlichen Änderungen an der NOVA-Plattform oberste Priorität.

Der Zugriff auf die operativen Rollen von NOVA Anbieter wird durch Gruppenmitgliedschaften im Active Directory (AD) der SBB gesteuert. Die Benutzerverwaltung (Erstellung, Löschung) oder die Passwörter werden somit direkt vom SBB-AD und nach den Regeln der SBB verwaltet. Kritische Rollen werden vom NOVA Partner Management Team verwaltet. Die neue Zuweisung einer kritischen Rolle wird nur mit Zustimmung des Vorgesetzten oder eines bekannten Teammitglieds vergeben. Einmal im Jahr wird die Notwendigkeit der Rolle erneut überprüft.

Als «kritische Rollen» werden alle Rollen betrachtet, die Änderungen mit finanziellen Auswirkungen ermöglichen, namentlich:

- Powertool Admin: diese Rolle bietet Zugriff auf die Funktionen des Tools zu den gewissen Mutationen von Kunden, Leistungen und Verträgen.
- TestClient: diese Rolle bietet Zugriff auf dem Testclient und ermöglicht, Vorgänge in NOVA Anbieter, wie z. B. Verkäufe, mit denselben Parametern wie ein bestimmter Vertriebskanal zu replizieren.
- Pflegetool: diese Rolle bietet Zugriff auf dem Pflegetool und die Möglichkeit, Stammdaten und Konfigurationen zu verwalten.
- Kontingente für Sparbillette: diese Rolle ermöglicht die Verwaltung von Sparbilleten. Unterrollen ermöglichen den Zugriff auf die Verwaltung von Sparbilletten der unterschiedlichen Leistungsvermittler.
- Neue Gutscheinwelt: diese Rolle ermöglicht die Verwaltung der Gutscheine und deren Kampagnen.

Technische Benutzerkonten sind erforderlich, um neue Softwareversionen einzusetzen, neue Daten zu verteilen und auf das System oder die Datenbank zuzugreifen.

Privilegien von externen Benutzern können durch bekannte Approver einzelner Transportunternehmen bestellt werden. Diese sind verantwortlich, dass die bestellten Mitarbeitenden angemessen sind, diese Privilegien zu haben und die SBB zu informieren, wenn diese Personen das Unternehmen verlassen/ eine andere Position im Unternehmen übernehmen, damit die SBB die Privilegien entzieht oder den AD Account deaktiviert.

3.8. Change-Management NOVA Anbieter

NOVA Anbieter wird nach den Grundsätzen der «agilen Softwareentwicklung» entwickelt. Dabei gilt es zwischen zwei unterschiedlichen Release-Szenarien zu unterscheiden:

- **Major Releases:** Ein «Major Version»-Produktionsrelease wird in der Regel alle 11 Wochen aufgeschaltet. Dies entspricht derzeit drei «Sprints» von sich ergänzenden Softwareanpassungen. Diese Releases enthalten grössere Änderungen an der Software, wie neue Features oder Anpassungen der Schnittstellen von NOVA Anbieter zu den Vertriebs- und Abrechnungssystemen. Aufgrund des Umfangs und der Vielfältigkeit der Änderungen, die mit einem Major Release in Produktion gesetzt werden, muss ein solcher Release entsprechend überprüft werden.
- **Minor Releases:** kleinere «Minor Version»/Patch-Releases werden je nach Bedarf in der Produktion aufgeschaltet. Solche Releases enthalten einerseits
  - nicht rechtzeitig fertiggestellte Änderungen, die für bereits aufgeschaltete Produktiv-Versionen von NOVA Anbieter benötigt werden und
  - Fehlerkorrekturen für Probleme, die in der Produktion festgestellt worden sind und kurzfristig korrigiert werden müssen.

Diese Änderungen werden ausserhalb des normalen Sprint-Modus nach Bedarf in die Produktion transportiert. Im Vergleich zu einem Major Release sind sie vom Umfang an Änderungen geringer und adressieren häufig nur spezifische Probleme. Diese Änderungen sind daher besser zu überblicken, können aber trotzdem erheblichen Einfluss auf die Finanzflüsse der öV-Branche haben.

Aufgrund der weitreichenden Auswirkungen von Anpassungen an der NOVA Anbieter Software durchlaufen alle diese Änderungen einen mehrstufigen Qualitätssicherungs- und Freigabeprozess. Wesentliche Komponenten bilden dabei:

- **Code-Review:** alle Änderungen werden technisch durch einen zweiten Entwickler geprüft und freigegeben, bevor sie in die Code-Basis für einen Produktionsrelease-Kandidaten integriert werden. Dazu wird mit dem «Pull Request»-Verfahren gearbeitet, welches technisch sicherstellt, dass der Code-Review nicht umgangen werden kann.
- **Fachliches Review:** alle Änderungen werden mit einer 4-Augenkontrolle durch eine fachlich versierte Person auf ihre Richtigkeit überprüft. Dieses fachliche Review ist organisatorisch verankert und kann teilweise auch mehrstufig sein.
- **Fachliche Regressionstests:** : In einem ersten Schritt wird nach der Fertigstellung eines Produktions-Release-Kandidaten für NOVA Anbieter ein umfassender fachlicher Regressionstest durchgeführt. Die notwendigen Regressionstests für die Prüfung, ob eine Änderung korrekt umgesetzt wurde, werden dabei von der fachverantwortlichen Person bereits vor der effektiven Umsetzung definiert und im jeweiligen Change Request festgehalten. Die Validierung und Freigabe der Regressionstestergebnisse erfolgten durch Tester auf Basis dieser Vorgaben. Diese Tester sind nicht in die Umsetzung (Programmierung) der Änderung involviert. Dadurch wird das 4-Augenprinzip für jede Änderung eingehalten. Nur bei durchgängiger Freigabe durch die zuständigen Tester wird ein Release-Kandidat von den Entwickler- auf die Test- und Integrationsumgebungen von NOVA portiert.
- Diverse weitere Fachtests, Regressions- und Lasttests der angeschlossenen Vertriebskanäle und der öV-Finanzsysteme werden bei Bedarf noch zusätzlich durchgeführt
- Der Release Manager erhält die Liste der Changes, die erfolgreich getestet wurden und erteilt die Freigabe für die Changes, die im Release deployed werden.

3.9. Stammdatenänderungen

Nicht die gesamte Tarif- und Abrechnungslogik ist in der Software von NOVA Anbieter verbaut. Ein grosser Teil davon, wie beispielsweise die Preisinformationen, für die über NOVA verkauften öV-Dienstleistungen oder auch die Verteilschlüssel, welche die Basis für die Ertragsverteilung der verkauften öV-Leistungen bilden, sind in den Stammdaten für NOVA Anbieter abgebildet.

Neue Tarif- und Abrechnungsdaten werden normalerweise im Wochenrhythmus in Produktion aufgeschaltet. Die Datenpflege-Organisation berücksichtigt dabei sowohl im normalen Bestellmodus bestellte Änderungen wie auch Daten-Bugfixes für kurzfristig in der Produktion aufgetauchte Probleme. Drei unterschiedliche Arten der Stammdatenpflege lassen sich dabei feststellen:

- **Tarifperiodenstandwechsel (TPS-Wechsel):** zweimal jährlich, am 1. Juni («kleiner Fahrplanwechsel») und Mitte Dezember («grosser Fahrplanwechsel»), existieren Fenster für grössere Anpassungen an den finanzrelevanten Stammdaten des öVs.
- Mit Bezug auf die NOVA Stammdaten fängt auf diese Stichdaten ein neuer Tarifperiodenstand an. Anpassungen der Tarife für den direkten Verkehr und die Verbunde – deren Produkte die überwältigende Mehrheit an Absatz- und Umsatzvolumen
  über NOVA ausmachen – werden zu diesen Zeitpunkten aufgeschaltet. Dazu gehören auch die «Tarifmassnahmen», welche die grossflächigen, durch den Preisüberwacher genehmigten Anpassungen der Basistarife des öV enthalten. Ebenso werden im Rahmen der TPS-Wechsels die grösseren abrechnungsrelevanten Anpassungen in den Stammdaten gemacht (wie beispielsweise Änderungen der Verteilschlüssel für die Erträge aus GA-Verkäufen oder DV-Tageskarten).
- **Wöchentliche Aktualisierung von Produkt- und Basisdaten:** Als Teil der wöchentlichen Datenrelease-Deployments in der Produktion werden folgende Änderungen an den Produkt- und Basisdaten vorgenommen:
  - Aufschaltung neuer Produkte auf NOVA. Die Aktivierung neuer Produkte auf NOVA ist nicht an die TPS-Wechsel gebunden.
  - Dazu gehört einerseits die Einführung neuer Angebote, die erstmals im öV verkauft werden (seit Betriebsbeginn von NOVA wurden beispielsweise das Modul-Abo oder die Spartageskarte aufgeschaltet). Anderseits gehört dazu auch die Migration von öV-Produkten, die zurzeit noch auf den «alten» Vertriebssystemen des öV laufen (für die SBB-
    Produkte beispielsweise Prisma, es gibt jedoch auch diverse Vertriebssysteme bei anderen TU, von denen Produkte migriert werden können). Diese Produkte sind zwar nicht «neu» im öV, aber müssen als neue Produkte in NOVA erfasst werden.
  - Änderungen an Preisen und Tarifen für die öV-Produkte der konzessionierten Transportunternehmen (KTU).
  - Aufschaltung von zeitlich beschränkten Sonderaktionen.
  - Fehlerkorrekturen für Produktionsprobleme.

Neben diesen Änderungen werden auch diversen nicht finanzwirksame Anpassungen in den Stammdaten gemacht, wie beispielsweise die Anpassung von Drucktexten.

- **Wöchentlicher Aktualisierung der Tarifnetze:** Die Tarifnetze sind die Basis für die Tarifierung aller streckenbasierten öV-Produkte. Sie legen die Preise für jede Strecke im Schweizer öV-Netz fest. Grundsätzliche Anpassungen an den Tarifnetzen werden im Rahmen der TPS-Wechsel gemacht. Als Teil der wöchentlichen Aufschaltung neuer Datenreleases müssen die Tarifnetze jedoch an kurzfristige Fahrplanänderungen, die beispielsweise aufgrund der Verschiebung von Haltestellen oder Streckensperrungen erfolgen, angepasst werden. Diese Anpassungen betreffen generell immer nur wenige oder teilweise sogar nur eine einzige Strecke. Zudem haben sie nie die Absicht, die Tarife aktiv anders zu gestalten. Nichtdestotrotz ist eine korrekte Angleichung der Tarifnetze an die Fahrplanänderungen wichtig, damit die betroffenen Strecken korrekt tarifiert werden.

3.10. Anteile

Zonenmodell

Im Zonenmodell werden die Umsätze immer zu 100% dem Tarifowner zugeteilt. Die Geschäftsführende konzessionierte Transportunternehmung (KTU) ist zuständig für Aufteilung der Anteile an die verschiedenen Leistungserbringer (teilnehmende KTUs).

Fixpreismodell

Die Anteile werden immer durch den Tarifowner bestimmt und bei NOVA-Datenmanagement (NOVA-DM) bestellt Die Anteilregeln können pro Produkt wie folgt definiert werden:

- Für das gesamte Produkte gültige Anteile
- Klassenabhängige, automatisch an Ausprägungen zugewiesene Leistungsanteile
- Manuell an Ausprägungen zugeordnete Leistungsanteile

Beispiele von Anteilen:

- 100% an Tarifowner
- Prozentsatz oder Fixbetrag
- Empfänger:
  - Partnerrolle wie z.B. den Leistungsvermittler
  - 1-n bestimmte KTU
  - 1-n Verteilschlüssel
- Rundung
- B2B-Rabatt (wird nur als Information geliefert)
- Provision (siehe unten)

Diese obigen Bespiele sind uneingeschränkt kombinierbar. Beispiel:
Produkt: «Swiss Travel Pass Flex 3 Tage»
Anteilregel «manuell an Ausprägung»: Ausprägung Vollpreis (Person 25+), 2. Klasse:
Anteile:

- Fixbetrag an Versteilschlüssel 118
- Fixbetrag an Verteilschlüssel 77
- Fixbetrag an KTU 918
- B2B Rabatt
- Verkaufsprovision Streckenabonnemente

Die Anteile pro Anteilregel Art im Prozent oder Betrag müssen 100% des Preises des Produkts ergeben.
Die Verteilschlüssel und deren Anpassungen werden durch Alliance SwissPass (ASP) berechnet und bei NOVA-DM bestellt.

DV-Modell
Im DV-Modell gibt es in der Preisberechnung zwei Arten von KTUs:

- mit Preisanstoss
- mit Kilometeranstoss: es werden alle Tarifwerte für diese KTUs aufaddiert (Relationsgruppe) und mittels der Tarif 601 (T601) Preistabelle dem Preis berechnet.

Entsprechend werden die Anteile unterschiedlich berechnet: Der Betrag wird proportional verteilt:

- KTUs mit Preisanstoss: der Betrag, welcher für die Strecke der jeweiligen KTU berechnet wurde.
- KTUs mit Kilometeranstoss: der errechnete Betrag aus der Preistabelle T601 wird proportional gemäss der jeweiligen Tarifwerte der KTUs in der Relationsgruppe verteilt.

Provisionen und Abzüge
Bei NOVA werden die Anteile vorerst zu 100% verteilt. Gibt es Abzüge wie Provisionen werden diese zurückgerechnet gemäss Finanzierer.
Z.B. bei der Provision DV-Einzelfahrausweise:

- Finanzierer: wie Leistungsanteile
- Empfänger: Leistungsvermittler

Beispiel:
Provision 12% (min CHF 1.00 / max CHF 5.00)
Betrag: CHF 30.00 verteilt an allen Empfänger 50% SBB – 50% BLS
Verkaufsstelle RBS
Provision: CHF 3.60 werden zu 50% SBB – 50% BLS belastet (je CHF 1.80) und der RBS zugeteilt.

3.11. Aufschaltung von Produkten und Kanälen

Für die Aufschaltung von Produkten und Kanälen wurden in Zusammenarbeit mit Alliance SwissPass verbindliche Abnahmekriterien definiert. Für die Abnahme ist das öV-Governance Team verantwortlich.

Jedes Produkt, welches erstmals über die NOVA Plattform angeboten werden soll, muss erfolgreich die Finanzcluster C1 und C2 durchlaufen (inkl. Stammdatenprüfung). Zur Erstellung der Prüfdaten werden (durch die Mandatierten definierte) Szenarien je Produkt über einen Testautomat (VGTP) am NOVA Anbieter gekauft. Über NOVA Abrechnung werden die Käufe je Produkt verdichtet (simulierter Monatsabschluss) und die öV-Leistungsabrechnung sowie das öV-Reporting erstellt.
Mandatierte, die durch ein öV- Gremium beauftragt sind, prüfen die Layoutvorgaben, die tarifliche Korrektheit und die finanziellen Aspekte.

Jeder Kanal, über den via NOVA Plattform Produkte verkauft werden sollen, muss erfolgreich die Finanzcluster C3 und C4 durchlaufen.

C1: Angebotsprüfung und Anteilsberechnung
Im Fokus dieser Abnahme ist das Produkt. Es wird geprüft, ob das Produkt auf NOVA richtig programmiert ist und die Anteile und Preise korrekt berechnet werden. Ausserdem wird verifiziert, ob die sonstigen Produktinformationen (Konditionstexte, Kundengruppen, Druckattribute, usw.) stimmen und die SAV Berechnung korrekt sind.

C2: öV-Abrechnung und öV-Reporting
Im Fokus dieser Abnahme ist die Abrechnung und das Reporting. Es wird geprüft, ob das Produkt auf NOVA richtig abgerechnet und rapportiert wird.

C3: Ticket-Erstellung und Layout
Im Fokus dieser Abnahme stehen die Belege. Belege können sein: Billette (E-Tickets/Screen-Tickets und Sicherheitspapier), Kaufquittungen (z.B. Abo auf SwissPass), SAV-Belege. Es wird geprüft ob die Belege fachlich und Layout technisch korrekt sind.

Das Layout wird gegenüber einem Referenzlayout geprüft. Die Kontrollelemente (z.B. Barcode, QR-Code, Referenzierung auf SwissPass) werden mit einem Kontrollgerät verifiziert. Bei Produkten auf SwissPass werden die SwissPass-spezifischen Prozesse End to End geprüft.

C4: Payment, Saldierung und Vertriebsbuchhaltung Im Fokus dieser Abnahme steht die Buchhaltung. Es wird geprüft, ob die Verkaufs- und Zahlungslogs jeder einzelnen Transaktion passen und ob die Dienststellenbuchhaltung in den entsprechenden Konten bebucht wurde.

Betriebliche Prozesse in NOVA Abrechnung & öV- Reporting

3.12. Übersicht Finanzplattform

NOVA Abrechnung (oder öV-Abrechnung) und öV-Reporting sind Teil der Finanzplattform. Die Finanzplattform ist eine auf SAP basierendes, eigenständiges Branchensystem, welche über einen standardisierte Finanzschnittstelle mit dem zentralen Vertriebssystem und dem Anbietersystem (NOVA Anbieter) verbunden ist. Sie wickelt sämtliche Vertriebsgeschäfte (Billette und Abonnements) der öV-Branche finanziell ab. Sie ist damit ein existenzieller Bestandteil der Vertriebsprozesse und gewährleistet weitgehend automatisiert und standardisiert die Einnahmesicherung und die Ertragsverteilung über 254 Transportunternehmen und 21 Verbünde des öffentlichen Verkehrs nach dem DV Teilmandat Abrechnung V512 der öV-Branche.

Der Service öV-Abrechnung & Reporting ist eine von insgesamt dreizehn betriebenen Services auf der Finanzplattform. Sie hat die Aufgabe, Verkehrserträge präzise für alle beteiligte Transportunternehmen abzurechen und ein entsprechendes Finanzreporting dazu bereitzustellen.
Die Finanzplattform wird durch die ART Financial Systems & Services (FSS) im agilen Entwicklungsmodus weiterentwickelt und betrieben.

3.13. Berechtigungsmanagement

SAP Access Control

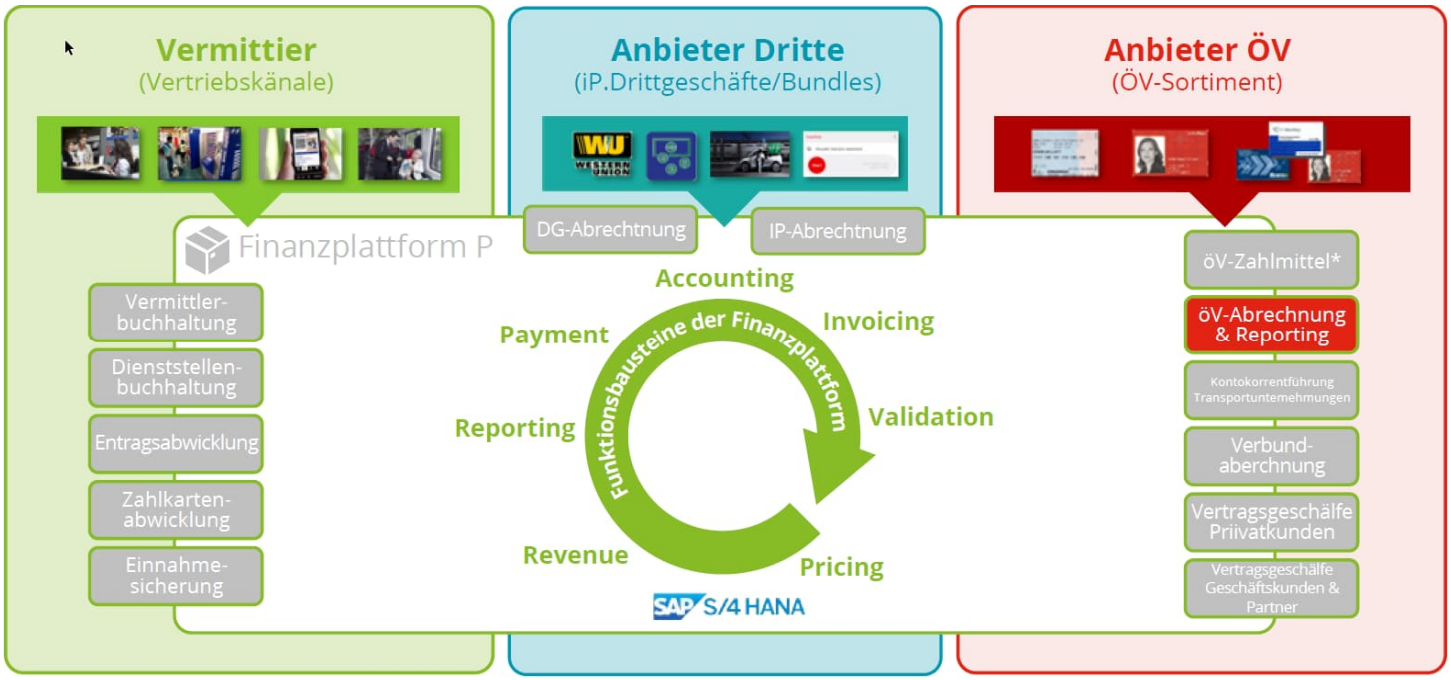
Die Finanzplattform enthält sensitive Finanz-, Unternehmens- und Personaldaten. Das Berechtigungsmanagement wird daher grundsätzlich durch den standardisierten SAP Access Control Prozess zur Verfügung gestellt und verwaltet.
Darin wird konsequent zwischen fachlichen und technischen Rollen unterschieden, welche durch ein mehrstufiges Genehmigungsverfahren durch einen Rollen-Eigner vergeben werden.

Fachliche Rollen

Fachliche Rollen werden durch den anwendungs-/ prozessverantwortlichen fachlichen Rollen-Eigner nach Prüfung des Antrages genehmigt.

Technische Rollen

Technische Rollen werden nach eingehender Prüfung des Antrages durch den Plattform-/Service verantwortlichen Systemarchitekten von FSS und/oder durch die Linienvertretung, welche eine entsprechende Fachdisziplin verantwortet (z.B. ABAP- Entwicklung), genehmigt.
Jedes FSS Mitglied unterzeichnet mit seinem Eintritt ein rechtlich bindendes Non-Disclosure Agreement (NDA).



3.14. Change Management – NOVA Abrechnung

Releaseplanung

FSS orientiert sich grundsätzlich an der Releaseplanung und den entsprechenden Releasezyklen von NOVA Anbieter. Die Releasedaten werden im Release-Kalender der DSO MKS gemeinsam geplant und geführt.

Beauftragung neuer Funktionalitäten

FSS setzt die neue Funktionalitäten gemäss den Anforderungen der Alliance SwissPass aus NOVA Anbieter oder aus regulatorischen Anforderungen auf NOVA Abrechnung um. Die laufende Umsetzung wird durch den gemeinsamen Verpflichtungskredit der Branche finanziert.

Anforderungsmanagement

FSS integriert sich in das Anforderungsmanagement von NOVA Abrechnung, unterhält aber einen spezifischen Product Backlog für die Finanzplattform. Mit NOVA zusammenhängende Anforderungen werden zusammen ausgearbeitet, verknüpft und geplant.

Abnahme & Testing

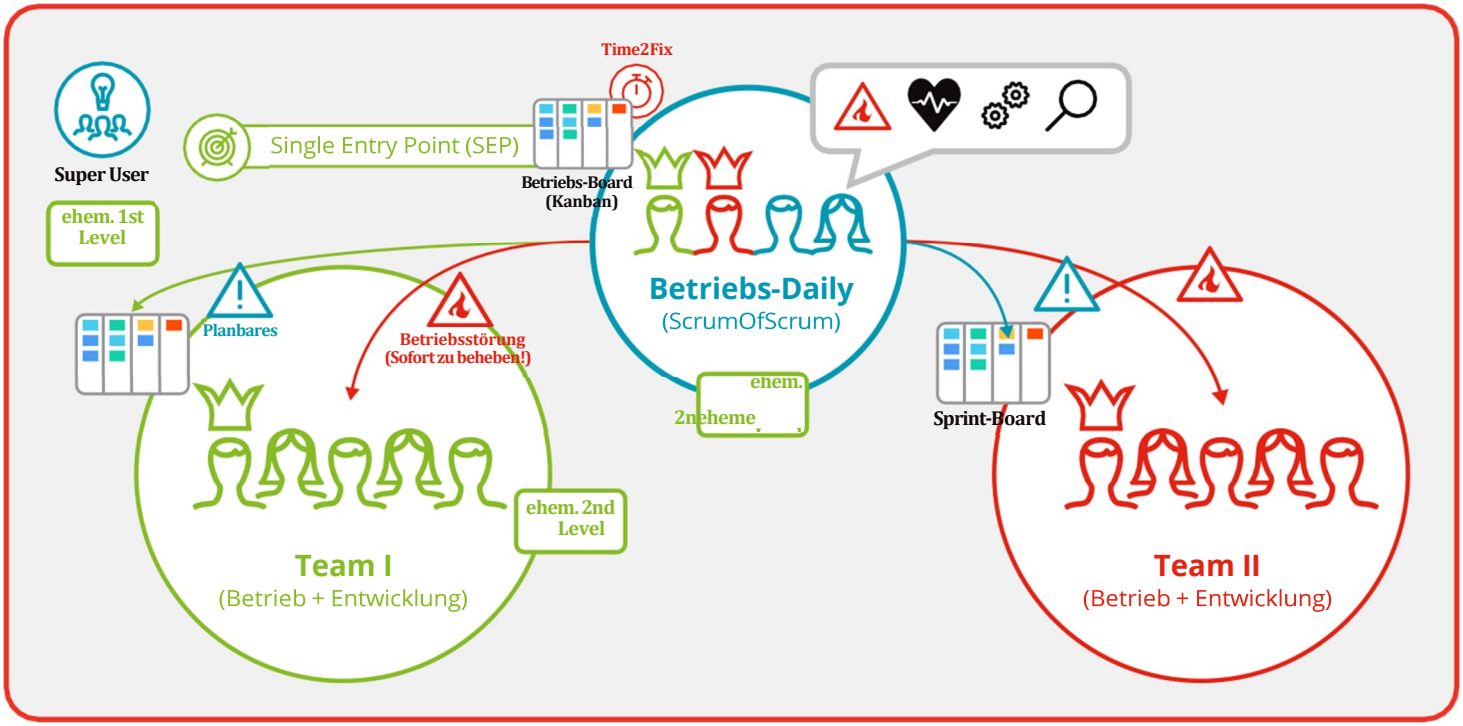
FSS integriert sich grundsätzlich am Abnahme- & Testprozess von NOVA Abrechnung stellt jedoch die auf der Finanzplattform umgesetzteTeilfunktionalität mit einem Vorlauf und einer Vorabnahme bereit. FSS führt die regulären Abnahmen auf einer vorproduktiven Stufe (Integerationsumgebung) mit NOVA Abrechnung durch. Bestehende Funktionalitäten werden durch automatisierte Financial Testing Framework (FIT) laufend überwacht und geprüft.

NOVA bindet die Funktionalität nachgelagert für das gemeinsame Abnahmetesting und der Produktivsetzung an. Die gemeinsamen Abnahmen unterliegen der Verantwortung der öV-Governance (siehe oben).

Fehlerbehebung

Alle Betriebsmeldungen werden zentral durch die Betriebsorganisation «Analyse & Triage» als Single-Entry-Point (SEP) der DSO MKS entgegengenommen und den entsprechenden Arbeitsorganisation zugewiesen. Die weiterführenden Analysen und die Klassifizierung der Meldungen wird durch die Arbeitsorganisation und dem entsprechenden Einbezug der Fachabteilungen sichergestellt.

Betriebsmeldungen werden in Betriebsstörungen (Major Incident, Incident) und Fehler (Defects) klassifiziert und gemäss Analyse und Triage (Priorisierung nach Triagekriterien) behoben. Major Incidents werden ad-hoc gelöst. Defects werden im ordentlichen Releasezyklus eingeplant und behoben.



Kontrollen durch die Leistungsvermittler und «Nullerprüfung»

3.15. Monatliche Kontrolle Umsatz durch Leistungsvermittler

Verschiedene Transportunternehmen haben mit der Einführung von NOVA als neue Vertriebsplattform eigene Verkaufskanäle an die NOVA-Plattform angebunden und verkaufen als Leistungsvermittler Produkte an ihre Kunden.

Ist ein NOVA-Kanal produktiv im Betrieb, müssen gemäss Vorgabe der Alliance SwissPass monatliche Kontrollen des Umsatzes aus der Verkaufsabrechnung mit der Belastung aus der öV-Leistungsabrechnung durchgeführt werden. Werden bei der Kontrolle Differenzen festgestellt, sind diese zu ermitteln, zu dokumentieren und zu bereinigen. Die NDV Revisionsstelle der Alliance SwissPass führt regelmässige Kontrollen bei den Leistungsvermittlern über die korrekte und vollständige Einlieferung und Abrechnung aller Verkäufe aus den NOVA Kanälen durch. Sie überprüft auch, dass die Abstimmung monatlich erfolgt und dokumentiert ist. Im Rahmen der NOVA-Plattform kann nicht geprüft werden, ob tatsächlich alle Verkäufe eingeliefert wurden. So sind beispielsweise Verkäufe von Geräten, die nicht ständig online sind (einzelne Automaten, Chauffeurverkauf etc.) erst ersichtlich, wenn diese über NOVA offline eingeliefert und abgerechnet sind.

3.16. Abgleich Verkäufe mit NOVA Leistungsabrechnung

Seitens NOVA Abrechnung wird täglich automatisiert geprüft, ob alle eingelieferten Verkäufe vollständig an die Leistungserbringer verteilt wurden. Dazu wird ein Abstimmbericht im öV-Reporting ausgeführt («Nullerprüfung»). Allfällige Fehler werden laufend abgearbeitet und im Rahmen des Monatsabschlusses wird durch das Mandat Abrechnung der Saldo 0.00 validiert und dokumentiert.

3.17. Ergänzende Benutzerentitätskontrollen

Bei der Entwicklung ihres Kontrollsystems hat die SBB in Betracht gezogen, dass bestimmte ergänzende Kontrollen von den Benutzereinheiten durchgeführt werden, um bestimmte in diesem Bericht genannte Kontrollziele zu erreichen. Die Transportunternehmen (User Entities) sind dafür verantwortlich, die Tools und Prozesse zu verstehen, die entweder von Mitarbeitenden der Kunden oder von SBB-Mitarbeitenden entwickelt wurden, für die sie verantwortlich sind und die sie unterstützen. Diese Lösungen, Prozesse und Tools gehören nicht zum Umfang dieses Berichts. Zu den Kontrollen, für die eine Benutzereinheit verantwortlich ist, gehören die folgenden:

Kontrollziel	Ergänzende Benutzerentitätskontrollen
Verteilschlüssel:	Der zugrundeliegende Verteilschlüssel für die inhaltlichen Kontrollen wird durch die Alliance SwissPass zur Verfügung gestellt und ist nicht Teil dieser Revision.
Kontrollziel 1:	Ausgetretenen Mitarbeitenden oder Mitarbeitenden, die für die User Entities arbeiten und keinen Zugriff mehr benötigen, werden an die SBB gemeldet, damit deren Zugriff zeitnah entfernt werden kann.
Kontrollziel 5:	Transportunternehmen melden alle Änderungen der SBB, damit diese umgesetzt werden können.

Kapitel IV: Kontrollziele, dazugehörige Kontrollen und Prüfung der Wirksamkeit der Kontrollen durch Deloitte

Kapitel IV: Kontrollziele, dazugehörige Kontrollen und Prüfung der Wirksamkeit der Kontrollen durch die externe Prüfgesellschaft

Einleitung

Dieser Abschnitt enthält die folgenden Informationen, welche von der SBB bereitgestellt werden:

- Die von SBB festgelegten Kontrollziele.
- Die Ausgestaltung und Implementierung der Kontrollen zur Erreichung der beschriebenen Kontrollziele.

Ebenfalls in diesem Abschnitt enthalten sind die folgenden Informationen der Deloitte AG:

- Eine Beschreibung der von der Deloitte AG durchgeführten Prüfungshandlungen, um festzustellen, ob die Kontrollen von SBB wirksam durchgeführt wurden, um die von ihnen festgelegten Kontrollziele zu erreichen. Die Deloitte AG hat Art, Zeitpunkt und Umfang der durchgeführten Prüfungshandlungen festgelegt.
- Die Resultate der von der Deloitte AG durchgeführten Prüfungshandlungen.

Im Rahmen der Prüfung von NOVA Abrechnung haben wir auch unterstützende Tools berücksichtigt und geprüft. Dies beinhaltet namentlich SAP GRC und SAP CUA für die Benutzerverwaltung sowie Streamworks für die Datenübermittlung und -verarbeitung in NOVA Abrechnung.

4.1 Zugriffsicherheit NOVA Anbieter

Kontrollziel 1 – Die Kontrollen stellen angemessen sicher, dass der Zugang zum NOVA Anbieter genehmigt wird und auf der Grundlage der Arbeitsfunktionen angemessen ist; Zugriffsrechte von gekündigten/ausgetretenen Benutzern zeitnahangepasst wird sowie die hochprivilegierten Accounts angemessen vergeben sind.

Kontroll-ID	Kontrollbeschreibung	Prüfungshandlung	Resultat
1.1	Zugriffsberechtigung Art und Umfang der Benutzerzugriffsrechte für neue und geänderte Benutzerzugriffe werden beantragt, genehmigt und im System implementiert.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Stichprobenbasierte Prüfung von vergebenen NOVA Anbieter Berechtigungen, um sicherzustellen, dass die Berechtigungen angefragt und von den Fachverantwortlichen genehmigt werden.	Bei 1 aus 25 überprüften neu vergeben oder modifizierten Zugriffsberechtigungen wurde eine Berechtigung ohne Beantragung und Genehmigung implementiert. Der Benutzer wurde im Rahmen der Rezertifizierung bestätigt und dessen Berechtigungen sind angemessen für die Verantwortlichkeiten des Benutzers.
1.2	Zugriffsentzug Ausgetretenen SBB-Mitarbeitenden wird der AD-Zugriff zeitnah entzogen. Die Gültigkeit der AD-Benutzer der Mitarbeitenden, die nicht für die SBB arbeiten, ist auf maximal 400 Tage beschränkt. Bei der Bestellung des Benutzers per Formular kann die Gültigkeit nicht mehr als 400 Tage betragen.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Stichprobenbasierte Prüfung von SBB-internen Austritten, um sicherzustellen, dass diese rechtzeitig von den Fachverantwortlichen der zuständigen Stelle mitgeteilt und deren Zugriffe entfernt werden. Inspektion des Bestellprozesses für externe Benutzer, um sicherzustellen, dass eine Bestellung mit einer Gültigkeit von mehr als 400 Tagen nicht möglich ist. Stichprobenbasierte Prüfung von externen Benutzern, um festzustellen, dass diese nicht länger als 400 Tage gültig sind.	Keine Abweichungen festgestellt.
1.3	Überprüfung der Benutzerzugriffsrechte Die kritischen Zugriffsberechtigungen werden jährlich überprüft.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der jährlichen Rezertifizierung, um sicherzustellen, dass sie eine vollständige und genaue Liste der Benutzer enthielt, dass sie ordnungsgemäss dokumentiert und von der zuständigen Leitung durchgeführt wurde, wobei eine angemessene Aufgabentrennung durchgesetzt wurde. Inspektion der jährlichen Rezertifizierung, um sicherzustellen, dass der kritische Systemzugriff rechtzeitig und in angemessener Weise geändert wird.	Keine Abweichungen festgestellt.

Kontroll-ID	Kontrollbeschreibung	Prüfungshandlung	Resultat
1.4	Authentifizierung Die Authentizifierung für den Zugriffauf NOVA Anbieter erfolgt per AD. Passworteinstellungen stellen sicher, dass der Zugang geschützt ist. Die Passwortparameter entsprechen mindestens den folgenden Kriterien: • Passwortlänge: 12 • Passwortkomplexität: aktiviert • Passwortablaufdatum: 90 Tage ausser dauerhaftem und sicherem Passwort • Passworthistorie: 18 • Fehlerhafte Versuche: 5	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der Default Domain Policy und Beurteilung, ob die Parameter gemäss den internen Passwortrichtlinien eingestellt sind.	Bei der Prüfung der Passworteinstellungen auf Active Directory Ebene (Domäne «sbb. ch»), haben wir festgestellt, dass die implementierten Passwortvorgaben nicht den internen Vorgaben der SBB oder der Praxis in der Industrie entsprechen: • Komplexität: Nicht aktiviert (Vorgabe SBB: Aktiviert) • Sperrung nach fehlgeschlagenen Anmeldeversuchen: 10 Versuche (Vorgabe SBB: 5 Versuche) • Automatische Entsperrung: 30 min (Vorgabe SBB: Manuelle Entsperrung) • Maximales Passwortalter: 180 Tage (Vorgabe SBB: 90 Tage) • Minimales Passwortalter: 0 Tage (Industrie: 1 Tag) Active Directory wird in NOVA Anbieter zur Single Sign-On Authentifizierung verwendet. Wir verstehen, dass die SBB an der Umsetzung der Passwortanforderungen gemäss SBB- Vorgaben arbeitet und inzwischen die Mehrheit aller Accounts diesen Anforderungen folgen.
1.5	Privilegierter Zugriff Der Zugriff auf kritische Rollen ist autorisiert und entsprechend eingeschränkt.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der Benutzer mit kritischem Zugang und Befragung der SBB Verantwortlichen für NOVA Anbieter sowie Überprüfung der Berufsbezeichnungen, um sicherzustellen, dass der Zugang auf angemessenes Personal beschränkt ist.	Keine Abweichungen festgestellt.

4.2. Zugriffsicherheit NOVA Abrechnung

Kontrollziel 2 – Die Kontrollen stellen angemessen sicher, dass der Zugang zum NOVA Abrechnung genehmigt wird und auf der Grundlage der Arbeitsfunktionen angemessen ist; Zugriffsrechte von gekündigten/ausgetretenen Benutzern zeitnahangepasst wird sowie die hochprivilegierten Accounts angemessen vergeben sind.

Kontroll-ID	Kontrollbeschreibung	Prüfungshandlung	Resultat
2.1	Zugriffsberechtigung Art und Umfang der Benutzerzugriffsrechte für neue und geänderte Benutzerzugriffe werden genehmigt.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Stichprobenbasierte Prüfung von vergebenen SAP Berechtigungen, um sicherzuzustellen, dass diese per Antrag angefragt und von den Fachverantwortlichen genehmigt wird.	Bei der stichprobenhaften Überprüfung von 25 neu vergebenen Berechtigungen für SAP-Systems, welches für NOVA Abrechnung verwendet wird wurden keine Abweichungen festgestellt. Bei der Prüfung des SAP-Systems, welches für NOVA Abrechnung verwendet wird, haben wir festgestellt, dass für eine Person eine Rolle nicht entfernt wurde, obwohl der Benutzer intern die IT SAP-Spezialisten-Stelle gewechselt hat. Die Rolle war angemessen für die vorigen Tätigkeiten des Benutzers.
2.2	Zugriffsentzug Ausgetretenen SBB-Mitarbeitenden wird der Zugriff auf SAP zeitnah entzogen. Die Gültigkeit der SAP-Benutzer der externen Mitarbeitenden ist auf maximal 400 Tage beschränkt.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Kritische Durchsicht des Austrittsprozesses, um sicherzustellen, dass dieser dokumentiert ist. Stichprobenbasierte Prüfung von SBB internen Austritten, um sicherzustellen, dass diese rechtzeitig von den Fachverantwortlichen der zuständigen Stelle mitgeteilt und deren Zugriff entfernt wird. Stichprobenbasierte Prüfung von externen Benutzern, um sicherzustellen, dass Zugriffe auf 400 Tage beschränkt sind.	Interne Mitarbeitende: Keine Abweichungen festgestellt. Bei einem 100% Abgleich aller Austritte von der HR-Liste mit den im System aktiven SAP-Benutzern stellten wir fest, dass keine der ausgetretenen Mitarbeitenden einen aktiven SAP-Account mehr besitzen. Externe Mitarbeitende: Bei der Prüfung des SAP-Systems, welches für NOVA Abrechnung verwendet wird, haben wir festgestellt, dass der Zugriff eines externen Mitarbeitenden nicht wie in den SBB Reglementen vorgeschrieben zeitnah deaktiviert wurde. Die Person besitzt zwei aktivierte SAP-Benutzerkonten, da diese zur SBB als interne Mitarbeitende wechselte und zusätzlich ein reguläres SAP-Benutzerkonto mit den identischen Privilegien erhielt. Wir haben festgestellt, dass der externe Benutzeraccount nach dem Wechsel nicht verwendet wurde. Bei der Überprüfung der Gültigkeitsdauer 100% aller externen SAP-Benutzern wurden Keine Abweichungen festgestellt.

Kontroll-ID	Kontrollbeschreibung	Prüfungshandlung	Resultat
2.3	Überprüfung der Benutzerzugriffsrechte Die kritischen Zugriffsberechtigungen werden regelmässig überprüft.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der jährlichen Rezertifizierung, um sicherzustellen, dass sie eine vollständige und genaue Liste der Benutzer enthielt, dass sie ordnungsgemäss dokumentiert und von der zuständigen Leitung durchgeführt wurde, wobei eine angemessene Aufgabentrennung durchgesetzt wird. Inspektion der jährlichen Rezertifizierung, um sicherzustellen, dass der kritische Systemzugriff rechtzeitig und in angemessener Weise geändert wird.	Es wurde keine Rezertifizierung in der Berichtsperiode durchgeführt, daher konnte die Kontrolle nicht geprüft werden.
2.4	Authentifizierung Passworteinstellungen stellen sicher, dass der Zugang geschützt ist. Die Passwortparameter entsprechen mindestens den folgenden Kriterien: • Passwortlänge: 12 • Passwortkomplexität: aktiviert • Passwortablaufdatum: 90 Tage ausser dauerhaftem und sicherem Passwort • Passworthistorie: 18 • Fehlerhafte Versuche: 5	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der SAP-Passwortparameter, um sicherzustellen, dass die Parameter gemäss den internen Passwortrichtlinien eingestellt sind. Inspektion der Default Domain Policy und Beurteilung, ob die Passwort Parameter gemäss den internen Passwortrichtlinien eingestellt sind., um sicherzustellen, dass diese angemessen sind.	Bei der Prüfung der Passworteinstellungen auf Active Directory Ebene (Domäne «sbb. ch»), haben wir festgestellt, dass die implementierten Passwortvorgaben nicht den internen Vorgaben der SBB oder der Praxis in der Industrie entsprechen: • Komplexität: Nicht aktiviert (Vorgabe SBB: Aktiviert) • Sperrung nach fehlgeschlagenen Anmeldeversuchen: 10 Versuche (Vorgabe SBB: 5 Versuche) • Automatische Entsperrung: 30min (Vorgabe SBB: Manuelle Entsperrung) • Maximales Passwortalter: 180 Tage (Vorgabe SBB: 90 Tage) • Minimales Passwortalter: 0 Tage (Industrie: 1 Tag) Active Directory wird in NOVA zur Single Sign-On Authentifizierung verwendet. Wir verstehen, dass die SBB an der Umsetzung der Passwortanforderungen gemäss SBB-Vorgaben arbeitet und inzwischen die Mehrheit aller Accounts diesen Anforderungen folgen.

Kontroll-ID	Kontrollbeschreibung	Prüfungshandlung	Resultat
2.5	Privilegierter Zugriff Der Zugriff auf kritische Berechtigungen ist autorisiert und entsprechend eingeschränkt.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion von kritischen Berechtigungen von SAP-Benutzern, um sicherzustellen, dass diese angemessen eingeschränkt sind.	Keine Abweichungen festgestellt.
2.6	Zugriffskonfiguration Die Passwörter der Standard-SAP-Benutzer wurden geändert und werden sicher verwahrt.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der Standardpasswörter für Standard-SAP-Benutzern, um sicherzustellen, dass diese in allen Mandanten geändert und entsprechend gesichert sind.	Keine Abweichungen festgestellt.
2.7	SAP_ALL und SAP_NEW Dialog und Service Benutzern sind keine SAP_ ALL oder SAP_NEW Profile dauerhaft zugeordnet. Temporärer SAP_ALL/ SAP_NEW Zugang wird angefragt, genehmigt und zeitnah entzogen.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion aller dauerhaft vergebenen SAP_ALL und SAP_NEW Profilen, um sicherzustellen, dass diese keinen Dialog und Service Benutzern dauerhaft zugeordnet sind. Inspektion aller temporär zugeordneten SAP_ALL und SAP_NEW Profilen, um sicherzustellen, dass diese angefragt, genehmigt und zeitnah entzogen werden.	Keine Abweichungen festgestellt.
2.8	Notfallberechtigungen Die Benutzung von Notfallberechtigungen werden protokoliert und bis spätestens am 15. Tag des Folgemonats überprüft.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion des Notfallbenutzer-Prozesses, um sicherzustellen, dass alle Benutzungen protokolliert werden. Inspektion aller Benutzungen von Notfallberechtigungen, um festzustellen, dass diese zeitnah überprüft werden.	Bei der Prüfung der Reviews von Notfallbenutzer-Protokollen haben wir folgendes festgestellt: • 3 Protokolle waren zum Prüfzeitpunkt noch nicht überprüft, obwohl diese zu überprüfen gewesen wären. Die 3 Protokolle wurden jedoch vom SAP-Verantwortlichen geprüft und als angemessen beurteilt. • 12 Protokolle wurden nicht zeitnah überprüft.

4.3. Change Management NOVA Anbieter

Kontrollziel 3 – Die Kontrollen stellen angemessen sicher, dass es keinen Mangel im Change Management der NOVA Anbieter gibt, die Qualität neuer Versionen gesichert ist und nur eine begrenzte Anzahl von autorisierten Mitarbeitenden Änderungen an der Software vornehmen können.

Kontroll-ID	Kontrollbeschreibung	Prüfungshandlung	Resultat
3.1	Aufgabentrennung Die Personen, welche die Software entwickelt haben, sind nicht in die Fachprüfung involviert.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Stichprobenbasierte Prüfung von Änderungen, um sicherzustellen, dass die Fachprüfung durch eine andere Person als den Entwicklern durchgeführt wird.	Keine Abweichungen festgestellt.
3.2	Testen und Freigabe Zum Zeitpunkt der Freigabe durch den Release Manager aller Major Releases gibt es keine produktionsverhindernden Mängel durch den Tester aus dem Fachbereich.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Stichprobenbasierte Prüfung von Änderungen, um festzustellen, ob die Major Releases durch den Release Manager freigeben werden und es keine verhindernden Mängel vor der Produktivsetzung gibt.	Keine Abweichungen festgestellt.
3.3	Fachprüfungen durchgeführt Für keine Software-Versionen von NOVA Anbieter, die in Produktion aktiviert werden, fehlen die notwendigen Fachprüfungen.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Stichprobenbasierte Prüfung von Änderungen, um sicherzustellen, dass für alle Software-Versionsänderungen von NOVA Anbieter Fachprüfungen vorgenommen werden.	Keine Abweichungen festgestellt.
3.4	Systemlandschaften Es existiert eine getrennte Entwicklungs-, Integrations- sowie Produktionsumgebung für NOVA Anbieter.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der Systemlandschaft, um sicherzustellen, dass es eine getrennte Entwicklungs-, Integrations- sowie Produktionsumgebung gibt.	Keine Abweichungen festgestellt.

4.4. Change Management Nova Abrechnung

Kontrollziel 4 – Die Kontrollen stellen angemessen sicher, dass es keinen Mangel im Change Management der NOVA Abrechnung gibt, die Qualität neuer Versionen gesichert ist und nur eine begrenzte Anzahl von autorisierten Mitarbeitenden Änderungen an der Software vornehmen können.

Kontroll-ID	Kontrollbeschreibung	Prüfungshandlung	Resultat
4.1	Testen von Änderungen SAP-Transporte werden getestet und genehmigt, bevor sie in die Produktionsumgebung übernommen werden.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Stichprobenbasierte Prüfung von SAP-Transporten, um sicherzustellen, dass diese vor der Produktivsetzung getestet und genehmigt werden.	Keine Abweichungen festgestellt.
4.2	Systemlandschaften Es existiert eine getrennte Entwicklungs-, Test- sowie Produktionsumgebung für NOVA Abrechnung.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der Systemlandschaft, um sicherzustellen, dass eine getrennte Entwicklungs-, Test- sowie Produktionsumgebung existiert.	Keine Abweichungen festgestellt.
4.3	Berechtigungen Mandats-/ Systemöffnungen Die SAP-Benutzer, die System- und Mandantenöffnungen vornehmen können, sind auf angemessene Personen beschränkt.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion aller SAP-Benutzer, die System- oder Mandantenöffnungen vornehmen können, um sicherzustellen, dass diese angemessen eingeschränkt sind.	Keine Abweichungen festgestellt.
4.4	System- und Mandantenöffnungen System- und Mandantenöffnungen sind auf ein Minimum beschränkt und werden zuvor genehmigt.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion aller System- und Mandantenöffnungen, um sicherzustellen, dass diese angemessen und genehmigt sind.	Keine Abweichungen festgestellt.
4.5	Transportberechtigungen Die SAP-Berechtigung, um Änderungen in die Produktion einzuspielen, ist auf angemessene Personen beschränkt.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion aller SAP-Benutzer, die die Berechnung haben, Änderungen in die Produktion einzuspielen, um sicherzustellen, dass diese angemessen eingeschränkt sind.	Keine Abweichungen festgestellt.
4.6	Debug Berechtigungen Debug Zugriff wird nicht dauerhaft in der Produktion vergeben.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion aller SAP-Benutzer, die Debug Berechtigungen haben, um sicherzustellen, dass diese nicht dauerhaft vergeben werden.	Keine Abweichungen festgestellt.

4.5. Stammdaten- und Vertriebskonfigurationsänderungen - NOVA Anbieter

Kontrollziel 5 – Die Kontrollen stellen angemessen sicher, dass es keinen Mangel in der Anpassung der finanzrelevanten Stammdaten in NOVA Anbieter gibt, die Qualität der Anpassungen gesichert ist und die Produkt- und Vertriebskonfigurationsanpassungen richtige Finanzflüsse generieren.

Kontroll-ID	Kontrollbeschreibung	Prüfungshandlung	Resultat
5.1	4-Augenprinzip bei wöchentlichen Datenrelease Alle Datenreleases, welche in die Produktion gelangen, werden durch eine Person, die nicht die Anpassung der finanzrelevanten Stammdaten gemacht hat, fachlich geprüft und freigegeben.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Stichprobenbasierte Prüfung von neuen Produkten, um sicherzustellen, dass die Fachprüfung durch eine andere Person durchgeführt wird als die Anpassung der finanzrelevanten Stammdaten. Stichprobenbasierte Prüfung von existierenden Produkten mit Änderungen, um sicherzustellen, dass die Fachprüfung durch eine andere Person durchgeführt wird als die Anpassung der finanzrelevanten Stammdaten.	Keine Abweichungen festgestellt.
5.2	4-Augen-Prinzip bei Mutationen zum Datenstandwechsel Für alle finanzrelevanten Datenmutationen im Rahmen der TPS-Wechsel wird geprüft, dass von den zuständigen Datenpflege-Teams eine durchgängige 4-Augenkontrolle durchgeführt wird.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der Konfiguration im System, um sicherzustellen, dass das System so aufgesetzt ist, dass eine Datenmutation im Rahmen vom TPS-Wechsel nicht von derselben Person erstellt und kontrolliert werden kann. Stichprobenbasierte Prüfung der internen Kontrolle, um sicherzustellen, dass Änderungen im 4-Augen-Prinzip durchgeführt werden.	Keine Abweichungen festgestellt.
5.3	Datenmutationsprüfung Das Datenmanagement-Team prüft die korrekte Umsetzung einer Stichprobe von 30 Mutationen pro Quartal an Streckensperrungen, Tarifnetz-Relationentarifmodell sowie im Tarifnetz-Verbundnetz. Prüfungsgegenstand ist, ob für diese Mutationen ein Angebot generiert und geprüft wird, sowie ob die Preisberechnung korrekt durchgeführt wird.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Stichprobenbasierte Prüfung der internen Kontrolle, um sicherzustellen, dass diese durchgeführt wird und die überprüften Streckensperrungen, Tarifnetz- Relationentarifmodell sowie Preisberechnung korrekt durchgeführt wurden.	Keine Abweichungen festgestellt.

Kontroll-ID	Kontrollbeschreibung	Prüfungshandlung	Resultat
5.4	Anteils- und Preiseberechnung Anteils- und Preiseberechnung aller neuen Produkte werden überprüft, um festzustellen, ob diese korrekt berechnet werden.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Stichprobenbasierte Prüfung von neuen Produkten (Zonen, Fixpreis, DV), um sicherzustellen, dass die Anteils- und Preisberechnung gemäss der Bestellung implementiert werden.	Keine Abweichungen festgestellt.
5.5	Vertriebskonfigurationänderung Die Verkaufs- und Zahlungslogs der Transaktionen nach einer Vertriebskonfigurationsänderung (Produkt, Kanal) sind korrekt und die Dienststellenbuchhaltung wird in den entsprechenden Konten bebucht.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Stichprobenbasierte Prüfung von Vertriebskonfigurationsänderungen, um sicherzustellen, dass die Verkaufs- und Zahlungslogs nach einer Änderung überprüft und an die Dienststellenbuchhaltung in die entsprechenden Konten gebucht werden.	Keine Abweichungen festgestellt.

4.6. Datenlieferung zu NOVA Abrechnung und öV-Reporting

Kontrollziel 6 – Die Kontrollen stellen angemessen sicher, dass über NOVA Anbieter verkaufte öV-Leistungen in NOVA Abrechnung eingeliefert werden und die öV-Reporting-Tabellen vollständig befüllt sind.

Kontroll-ID	Kontrollbeschreibung	Prüfungshandlung	Resultat
6.1	Einlieferung zu NOVA Abrechnung Die Übertragung aller Leistungen von NOVA Anbieter an NOVA Abrechnung wird täglich und automatisch geprüft. Sollte eine Leistung nicht übertragen werden, wird dieser Fehler täglich wieder rapportiert, bis die Leistung korrekt übertragen wird. Das NOVA Partnermagement-Team stellt sicher, dass der Fehler korrigiert und alle Leistungen übertragen werden.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der Schnittstelle, um sicherzustellen, dass diese überwacht wird und keine unbegründeten Fehler beinhaltet. Inspektion der Arbeitsanweisung, um sicherzustellen, dass diese die Überwachung der Schnittstelle beinhaltet.	Keine Abweichungen festgestellt.
6.2	Befüllung der öV-Reporting Die Befüllung aller Leistungen innerhalb NOVA Abrechnung/öV-Reporting wird täglich und automatisch in Streamworks geprüft. Abbrüche werden zeitnah bearbeitet, Fehler korrigiert und Übertragungen neu gestartet.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der Streamworks Jobs, um sicherzustellen, dass sie täglich ausgeführt werden. Inspektion einer Stichprobe von Abbrüchen, um sicherzustellen, dass diese zeitnah bearbeitet, Fehler korrigiert und Übertragungen neu gestartet werden.	Keine Abweichungen festgestellt.
6.3	Vollständige Verteilung der Verkäufe Ein Abstimmbericht «Nullerprüfung» wird im öV-Reporting monatlich ausgeführt, um zu prüfen, ob alle eingelieferten Verkäufe vollständig an die Leistungserbringer verteilt wurden. Allfällige Fehler werden laufend abgearbeitet und im Rahmen des Monatsabschlusses wird durch das Mandat Abrechnung der Saldo 0.00 validiert und dokumentiert.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion des Abstimmungsberichtes «Nullerprüfung», um sicherzustellen, dass allfällige Fehler laufend abgearbeitet wurden und im Rahmen des Monatsabschlusses durch das Mandat Abrechnung der Saldo 0.00 validiert und dokumentiert wurde.	Keine Abweichungen festgestellt.
6.4	Authentifizierung Die Authentifizierung für den Zugriffauf Streamworks erfolgt per AD. Passworteinstellungen oder lokalen Authentifizierung (Technische Benutzer) und stellen sicher, dass der Zugang geschützt ist.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der Default Domain Policy und Beurteilung, ob die Parameter gemäss den internen Passwortrichtlinien eingestellt sind.	Bei der Prüfung der Passworteinstellungen auf Active Directory Ebene (Domäne «sbb.ch»), haben wir festgestellt, dass die implementierten Passwortvorgaben nicht den internen Vorgaben der SBB oder der Praxis in der Industrie entsprechen: • Komplexität: Nicht aktiviert (Vorgabe SBB: Aktiviert)

	Die Passwortparameter entsprechen mindestens den folgenden Kriterien: Passwortlänge: • Passwortlänge: 12 • Passwortkomplexität: aktiviert • Passwortablaufdatum: 90 Tage ausser dauerhaftem und sicherem Passwort • Passworthistorie: 18 • Fehlerhafte Versuche: 5	Inspektion der lokalen Passworteinstellung und Beurteilung, ob die Parameter gemäss den internen Passwortrichtlinien eingestellt sind sofern technisch möglich. Stichprobenbasierte Prüfung von Benutzern, ob diese der korrekten Authentifizierungsmethode zugeorndet sind.	• Sperrung nach fehlgeschlagenen Anmeldeversuchen: 10 Versuche (Vorgabe SBB: 5 Versuche) • Automatische Entsperrung: 30min (Vorgabe SBB: Manuelle Entsperrung) • Maximales Passwortalter: 180 Tage (Vorgabe SBB: 90 Tage) • Minimales Passwortalter: 0 Tage (Industrie: 1 Tag) Active Directory wird in NOVA zur Single Sign-On Authentifizierung verwendet. Wir verstehen, dass die SBB an der Umsetzung der Passwortanforderungen gemäss SBB Vorgaben arbeitet und inzwischen die Mehrheit aller Accounts diesen Anforderungen folgen. Alle überprüften Benutzer sind der korrekten Authentifizierung zugeordnet.
6.5	Privilegierter Zugriff Der Zugriff auf kritische Berechtigungen ist autorisiert und entsprechend eingeschränkt.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion von kritischen Berechtigungen von Streamworks-Benutzern, um sicherzustellen, dass diese angemessen eingeschränkt sind.	Keine Abweichungen festgestellt.
6.6	Zugriff auf Stream-Planung Der Zugriff auf nicht eigene Streams sowie deren Einplanung zu modifizieren ist autorisiert und entsprechend eingeschränkt.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion von Stream Berechtigungen von Streamworks-Benutzern, um sicherzustellen, dass diese angemessen eingeschränkt sind.	Keine Abweichungen festgestellt.
6.7	Streamwork Monitoring In Streamworks wird der erfolgreiche Abschluss der Streams überwacht und fehlgeschlagene Streams werden bei Bedarf erneut durchgeführt.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion des Streamworks Monitoring Dashboards, um sicherzustellen, dass der erfolgreiche Abschluss hin überwacht werden, und fehlgeschlagene Streams bei Bedarf erneut gestartet werden. Inspektion aller relevanten Streams um sicherzustellen, dass die Stream-Verantwortlichen über einen Stream Abbruch informiert werden.	Keine Abweichungen festgestellt.

4.7. Backup

Kontrollziel 7 – Die Kontrollen stellen angemessen sicher, dass NOVA Abrechnung nach einem Katastrophenfall wieder erstellt werden kann.

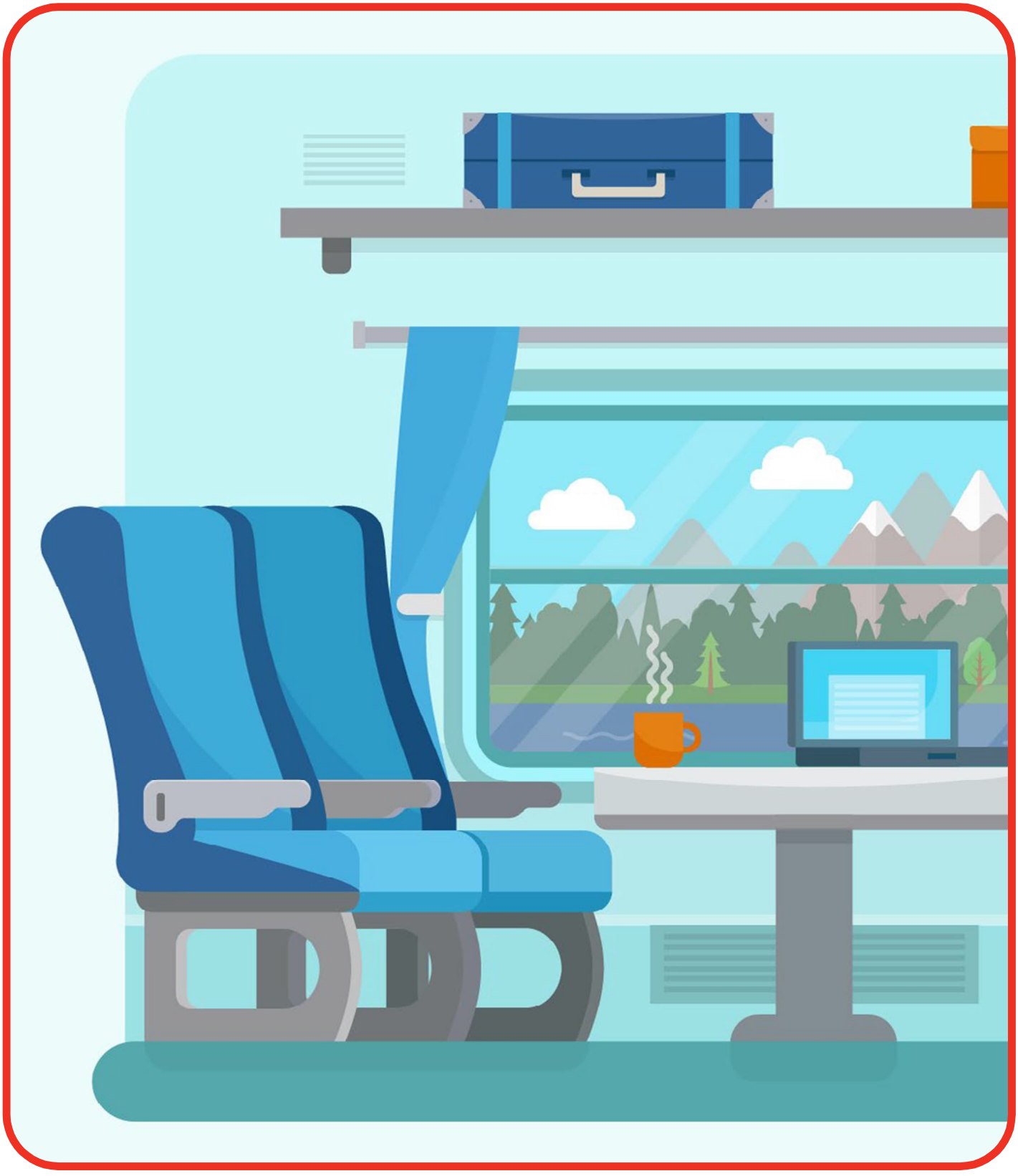
Kontroll-ID	Kontrollbeschreibung	Prüfungshandlung	Resultat
7.1	Erstellung von Backups Die Finanzdaten werden nach einem festgelegten Zeitplan in regelmässigen Abständen gesichert.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der Backup-Konfigurationen, um sicherzustellen, dass die Backups auf den Servern gemäss den SBB-Richtlinien angestossen werden.	Keine Abweichungen festgestellt.
7.2	Backup Monitoring Backup-Prozesse werden auf ihre erfolgreiche Ausführung überwacht. Fehler werden eskaliert und korrigiert, um sicherzustellen, dass die Daten nutzbar sind und bei Bedarf abgerufen und wiederhergestellt werden können.	Befragung der Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Inspektion der Backup-Prozesse, um sicherzustellen, dass die Ausführung überwacht, wird und relevante Fehler eskaliert werden. Inspektion eines Restore-Tests, um sicherzustellen, dass ein solcher während dem Berichtszeitraum erfolgreich durchgeführt wird.	Keine Abweichungen festgestellt.

4.8. ISAE-Berichte von Dienstleistern

Kontrollziel 8 – Die Kontrollen stellen angemessen sicher, dass die Sicherheit der Informationssysteme regelmässig revidiert werden. Die ISAE- Berichte relevanter Dienstleister werden geprüft, Bemerkungen zu Complementary User Entity Controls werden auf möglichen IKS-Einfluss geprüft und allfällige Anpassungen am IKS IT vorgenommen.

Kontroll-ID	Kontrollbeschreibung	Prüfungshandlung	Resultat
8.1	Die Resultate des für die NOVA Anbieter und NOVA Abrechnung relevanten ISAE3402-Berichts werden jährlich bezogen und eingesehen. Es wird geprüft, ob die zugehörigen Kontrollziele und Kontrollen der Serviceorganisation angemessen erreicht wurden, Observationen sowie die Complementary User Entity Controls für relevante Kontrollen identifiziert und allfällige Abweichungen beurteilt wurden.	Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird. Durch Einsichtnahme in die relevanten Unterlagen für den Bericht des Drittanbieters haben wir geprüft, ob die SBB einen Bericht unter anderem von T-Systems erhalten und die relevanten Kontrollziele und Kontrollen sowie allfällige Abweichungen beurteilt hat.	Keine Abweichungen festgestellt.

Kapitel V: Sonstige Informationen durch SBB



Kapitel V: Sonstige Informationen durch SBB

Die in Kapitel V dieses Berichts enthaltenen Informationen werden von SBB dargelegt, um dem Kunden zusätzliche Informationen zu liefern. Diese Informationen sind nicht Teil der Beschreibung des dienstleistungsbezogen internen Kontrollsystems durch SBB. Die in Kapitel V enthaltenen Informationen wurden nicht bei der Prüfung des dienstleistungsbezogen internen Kontrollsystems berücksichtigt. Dementsprechend gibt Deloitte darüber kein Urteil ab.

Kontroll-ID	Kontrollbeschreibung	Resultat	Management Stellungsname
1.1	Zugriffsberechtigung Art und Umfang der Benutzerzugriffsrechte für neue und geänderte Benutzerzugriffe werden beantragt, genehmigt und im System implementiert	Bei 1 aus 25 überprüften neu vergeben oder modifizierten Zugriffsberechtigung wurde eine Berechtigung ohne Beantragung und Genehmigung implementiert. Der Benutzer wurde im Rahmen der Rezertifizierung bestätigt und dessen Berechtigungen sind angemessen für die Verantwortlichkeiten des Benutzers.	Implementierte, mitigierende Sicherheitsmassnahmen Das Pflegetool wurde dieses Jahr erweitert, um dden Verbunden und TU zu ermöglichen, ihre Sparbilletekontingen selbst zu bearbeiten. Der Zugriff dieses Benutzers (auf dem Kontingent seiner TU) wurde in der Pilotphase mündlich bestätigt ohne dass eine dokumentierte Bestätigung ausgelöst wurde. Bereits umgesetzte Sofortmassnahmen Die Mitarbeitenden wurden auf die strenge Einhaltung des Prozesses erneut hingewiesen und geschult.
2.1	Zugriffsberechtigung Art und Umfang der Benutzerzugriffsrechte für neue und geänderte Benutzerzugriffe werdengenehmigt.	Bei der Prüfung des SAP-Systems, welches für NOVA Abrechnung verwendet wird, haben wir festgestellt, dass für eine Person eine Rolle nicht entfernt wurde, obwohl der Benutzer intern die IT SAP-Spezialisten-Stelle gewechselt hat. Die Rolle war angemessen für die vorigen Tätigkeiten des Benutzers.	Implementierte, mitigierende Sicherheitsmassnahmen Es gibt einen jährlichen Regelprozess, der die Berechtigungen überprüft und nicht mehr benötigte Berechtigungen entfernt. Bereits umgesetzte Sofortmassnahmen Dem Benutzer wurde die Rolle entzogen.
2.2	Zugriffsentzug Ausgetretenen SBB- Mitarbeitendenwird SAP zeitnah entzogen. Die Gültigkeit der SAP-Benutzer dere externen Mitarbeitenden ist auf 400 Tage beschränkt.	Interne Mitarbeitende: Bei der Prüfung des SAP-Systems, welches für NOVA Abrechnung verwendet wird, haben wir festgestellt, dass der Zugriff eines externen Mitarbeitenden nicht wie in den SBB Reglementen vorgeschrieben zeitnah deaktiviert wurde. Die Person besitzt zwei aktivierte SAP-Benutzerkonten, da diese zur SBB als interne Mitarbeitende wechselte und zusätzlich ein reguläres SAP-Benutzerkonto mit den identischen Privilegien erhielt. Wir haben jedoch festgestellt, dass der externe Benutzeraccount nach dem Wechsel nicht verwendet wird. Externe Mitarbeitende: Keine Abweichungen festgestellt.	Implementierte, mitigierende Sicherheitsmassnahmen Die Hierarchieverknüpfung verhindert einen Missbrauch. Es gibt einen jährlichen Regelprozess, der die Berechtigungen überprüft und nicht mehr benötigte Berechtigungen entfernt. Bereits umgesetzte Sofortmassnahmen Dem Benutzer wurde die Rolle entzogen.

2.3	Überprüfung der Benutzerzugriffsrechte Die kritischen Zugriffsberechtigungen werden regelmässig überprüft.	Es wurde keine Rezertifizierung in der Berichtsperiode durchgeführt, daher konnte die Kontrolle nicht geprüft werden.	Anmerkung SBB Die Überprüfung der Zugriffsberechtigungen wurde im Oktober 2022 initiiert und ist inzwischen abgeschlossen. Die SBB werden die Ergebnisse der Überprüfung mit Deloitte teilen. SBB plant im Januar 2023, zusammen mit dem Bridge Letter, einen Bericht (Agreed upon Procedures) nach PS 920 der Deloitte zur Verfügung zu stellen, in welchem die Prüfungshandlungen zur Kontrolle «Überprüfung der Benutzerzugriffsrechte» dargelegt werden.
1.4/2.4/6.4	Authentifizierung Passwort Einstellungen stellen sicher, dass der Zugang geschützt ist. Die Passwortparameter entsprechen mindestens der folgenden Kriterien: • Passwortlänge: 12 • Passwortkomplexität: aktiviert • Passwortablaufdatum: 90 Tage ausser dauerhaftem und sicherem Passwort • Passworthistorie: 18 • Fehlerhafte Versuche: 5	Bei der Prüfung der Passworteinstellungen auf Active Directory Ebene (Domäne «sbb.ch»), haben wir festgestellt, dass die implementierten Passwortvorgaben nicht den internen Vorgaben der SBB oder der Praxis in der Industrie entsprechen: • Komplexität: Nicht aktiviert (Vorgabe SBB: Aktiviert) • Sperrung nach fehlgeschlagenen Anmeldeversuchen: 10 Versuche (Vorgabe SBB: 5 Versuche) • Automatische Entsperrung: 30min (Vorgabe SBB: Manuelle Entsperrung) • Maximales Passwortalter: 180 Tage (Vorgabe SBB: 90 Tage) • Minimales Passwortalter: 0 Tage (Industrie: 1 Tag) Active Directory wird in NOVA zur Single Sign-On Authentifizierung verwendet. Wir verstehen, dass die SBB an der Umsetzung der Passwortanforderungen gemäss SBB Vorgaben arbeitet und inzwischen die Mehrheit aller Accounts diesen Anforderungen folgen.	Implementierte, mitigierende Sicherheitsmassnahmen Es handelt sich hierbei um ein SBB- und kein NOVA-spezifisches Thema. Mit dem SBB-internen Projekt OMADA wird dies bis Ende 1. Quartal 2023 umgesetzt.
2.8	Notfallberechtigungen Die Benutzung von Notfall Berechtigungen werden protokoliert bis maximal vom 15. des Folgemonats überprüft.	Bei der Prüfung der Reviews von Notfallbenutzer-Protokollen haben wir folgendes festgestellt: 3 Protokolle waren zum Prüfzeitpunkt noch nicht überprüft, obwohl diese zu überprüfen gewesen wären. Die 3 Protokolle wurden von dem SAP Verantwortlichen geprüft und als angemessen beurteilt. 12 Protokolle wurden nicht zeitnah überprüft.	Implementierte, mitigierende Sicherheitsmassnahmen In der Zwischenzeit wurden alle Protokolle bestätigt. Bereits umgesetzte Sofortmassnahmen Zur Verhinderung weiterer offener Protokolle wurde die bestehende IKS-Kontrolle überprüft und angepasst. Gleichzeitig wurde der Control Owner instruiert, die zeitnahe Bestätigung der Protokolle einzufordern.

Designed by CoReCreative Services. RITM1180078