



## 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. Oktober 2023 bis 30. September 2024



## Abkürzungsverzeichnis

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

# Inhaltsverzeichnis

|                                                                                                                                       |    |
|---------------------------------------------------------------------------------------------------------------------------------------|----|
| <b>Kapitel I:</b> Bericht der unabhängigen Prüfgesellschaft über die Beschreibung der Kontrollen, deren Ausgestaltung und Wirksamkeit | 03 |
| <b>Kapitel II:</b> Erklärung des Dienstleisters zum internen Kontrollsystem                                                           | 06 |
| <b>Kapitel III:</b> Beschreibung des internen Kontrollsystems                                                                         | 09 |
| <b>Kapitel IV:</b> Kontrollziele, dazugehörige Kontrollen und Prüfung der Wirksamkeit der Kontrollen durch Deloitte                   | 21 |
| <b>Kapitel V:</b> Sonstige Informationen durch SBB                                                                                    | 39 |



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



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

### An das Management der Schweizerischen Bundesbahnen AG

#### 1.1 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. Oktober 2023 bis zum 30. September 2024 (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.

SBB nutzt Dienstleistungen, die von der T-Systems erbracht werden. Die Beschreibung in Kapitel III umfasst nur die Kontrollen und zugehörigen Kontrollziele der SBB und schliesst die Kontrollziele und zugehörigen Kontrollen der T-Systems aus. Die Beschreibung weist auch darauf hin, dass bestimmte von SBB vorgegebene Kontrollziele nur dann erreicht werden können, wenn ergänzende Kontrollen der Subdienstleistungsorganisation, die bei der Konzeption der Kontrollen der Dienstleistungserbringer angenommen werden, zusammen mit den zugehörigen Kontrollen von der T-Systems angemessen konzipiert sind und wirksam funktionieren. Unsere Prüfung erstreckte sich nicht auf die Kontrollen der Subdienstleistungsorganisation oder deren Funktion und wir haben die Angemessenheit des Designs oder die operative Wirksamkeit dieser ergänzenden Kontrollen der Subdienstleistungsorganisation nicht beurteilt.

#### 1.2 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.

#### 1.3 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 ethischen Ansprüchen, beruflichen Verhaltensanforderungen und den anwendbaren rechtlichen und regulatorischen Vorschriften.

#### 1.4 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 organisation», 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. Oktober 2023 bis zum 30. September 2024.

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.

## 1.5 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 Prüfungsergebnisse 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.

## 1.6 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:

- Nach unserer Beurteilung und basierend auf den in der Erklärung der 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. Oktober 2023 bis zum 30. September 2024 sachgerecht wieder.
- Sofern die beschriebenen Kontrollen im Zeitraum vom 1. Oktober 2023 bis zum 30. September 2024 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.
- Die geprüften Kontrollen waren, bis auf die Abweichungen notiert in Kapitel 4, im Zeitraum vom 1. Oktober 2023 bis zum 30. September 2024 wirksam. Die geprüften Kontrollen entsprachen denjenigen Kontrollen, die zur Erreichung der in der Beschreibung enthaltenen Kontrollziele, auf der Basis einer angemessenen Sicherheit, notwendig waren.

## 1.7 Beschreibung der Prüfungshandlungen

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

## 1.8 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. Daher ist der Bericht, einschliesslich der Beschreibung der Kontrollen und der Management Stellungnahmen, ausschliesslich zur Information von SBB für die Berichterstattung über die Kontrolltätigkeiten der Serviceorganisation in Bezug auf die Ausgestaltung und Wirksamkeit der Serviceorganisation während eines Teils oder der Gesamtheit des Zeitraums vom 1. Oktober 2023 bis 30. September 2024 in Übereinstimmung mit den Bedingungen des Auftragsschreibens zwischen der Dienstleistungsorganisation und der Deloitte AG bestimmt.

Der Bericht darf ohne unsere ausdrückliche vorherige schriftliche Genehmigung weder ganz noch teilweise in einem anderen Dokument zitiert oder erwähnt werden, noch darf er einer anderen Partei zur Verfügung gestellt, kopiert oder zitiert werden, egal unter welchen Umständen.

Wir gestatten die Offenlegung dieses Berichts in vollem Umfang, einschliesslich der Beschreibung der Tests von Kontrollaktivitäten und ihrer Ergebnisse, durch SBB an die Mitglieder der Alliance SwissPass, die ihre Dienstleistungen im Bereich NOVA während einem Teil oder dem gesamten Zeitraum von 1. Oktober 2023 bis zum 30. September 2024 in Anspruch genommen haben, und deren Abschlussprüfer, die über ein ausreichendes Verständnis verfügen, um diese Informationen zusammen mit anderen Informationen, einschliesslich Informationen über die von den Kunden selbst durchgeführten Kontrollen, bei der Beurteilung des Risikos wesentlicher falscher Angaben in den Abschlüssen der Kunden zu berücksichtigen, um diese Parteien in die Lage zu versetzen, sich zu vergewissern, dass ein Bericht des Dienstleistungsprüfers von SBB in Auftrag gegeben und im Zusammenhang mit den Kontrollaktivitäten SBB erstellt wurde, ohne dass wir eine Verantwortung oder Haftung gegenüber diesen Parteien übernehmen oder akzeptieren.

Dieser Bericht ist nicht für die Verwendung durch andere als die genannten Parteien bestimmt und sollte auch nicht von diesen verwendet werden. Soweit dies gesetzlich zulässig ist, übernehmen wir gegenüber niemandem ausser SBB eine Verantwortung für unsere Arbeit, diesen Bericht oder die Schlussfolgerungen, die wir gezogen haben.

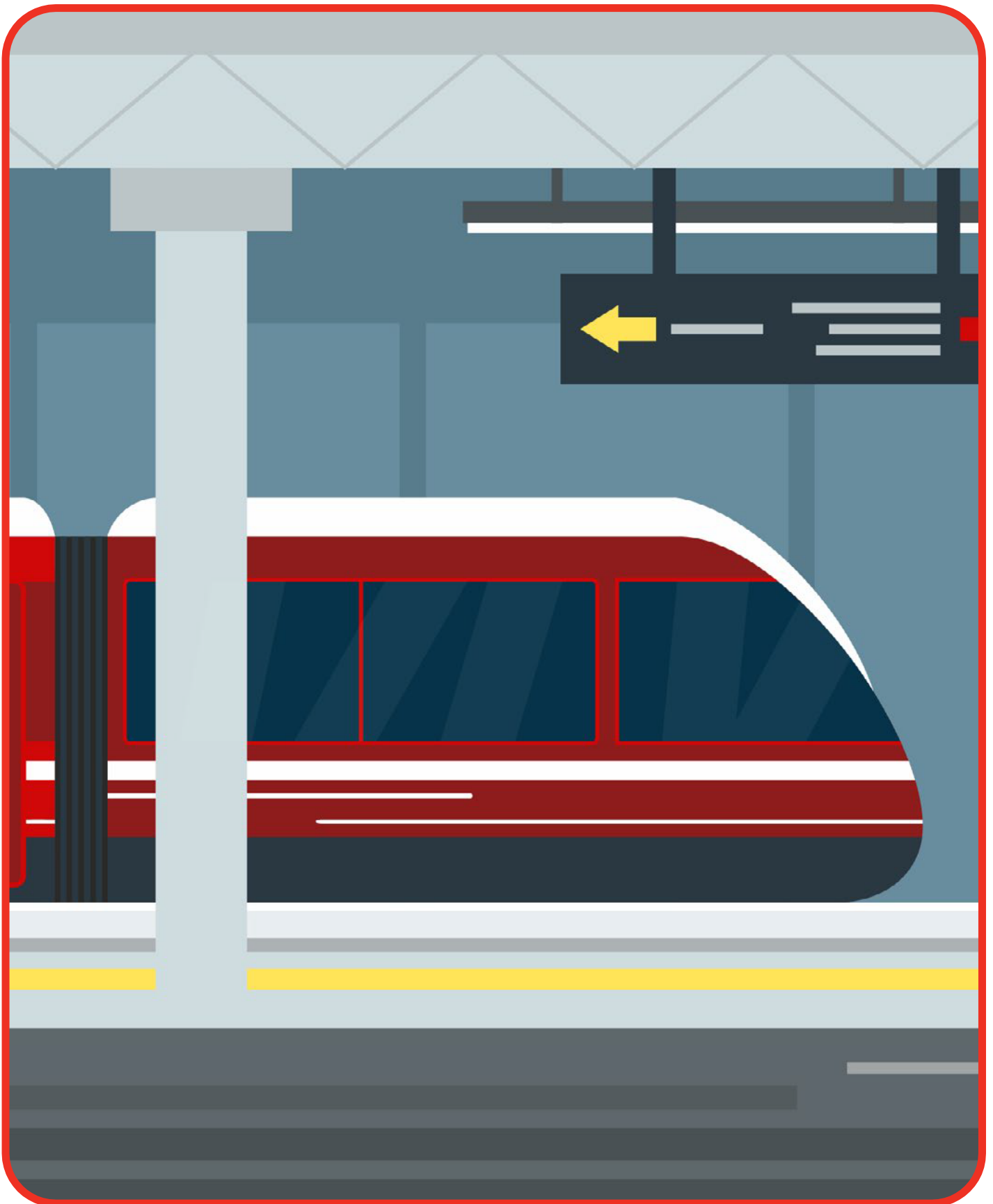
Deloitte AG

Fabien Lussu  
Partner

Simon Brander  
Director

Zürich, 20. Dezember 2024

## 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

### 2.1 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. Oktober 2023 bis zum 30. September 2024 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.

In der Beschreibung wird darauf hingewiesen, dass bestimmte von SBB vorgegebenen Kontrollziele nur dann erreicht werden können, wenn ergänzende Kontrollen des Dienstleistungsbezüger T-Systems, die bei der Konzeption der Kontrollen von SBB angenommen werden, zusammen mit den entsprechenden Kontrollen angemessen konzipiert sind und wirksam funktionieren. Die Effektivität der Kontrollen werden durch die SBB regelmässig überprüft.

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.

### 2.2 Beschreibungskriterien

Wir bestätigen nach bestem Wissen, dass:

- 1) die beiliegende Beschreibung des Kontrollsystems der NOVA-Umgebung («System») des Dienstleistungsempfängers in der Berichtsperiode vom 1. Oktober 2023 bis zum 30. September 2024 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. Oktober 2023 bis zum 30. September 2024 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. Oktober 2023 bis zum 30. September 2024 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. Oktober 2023 bis zum 30. September 2024 beschreibungskonform durchgeführt wurden. Dies beinhaltet, dass die manuellen Kontrollen nur durch solche Mitarbeitenden durchgeführt wurden, die dazu befähigt und berechtigt sind.

Schweizerische Bundesbahnen SBB,

**Monika Kaiser Zengaffinen**

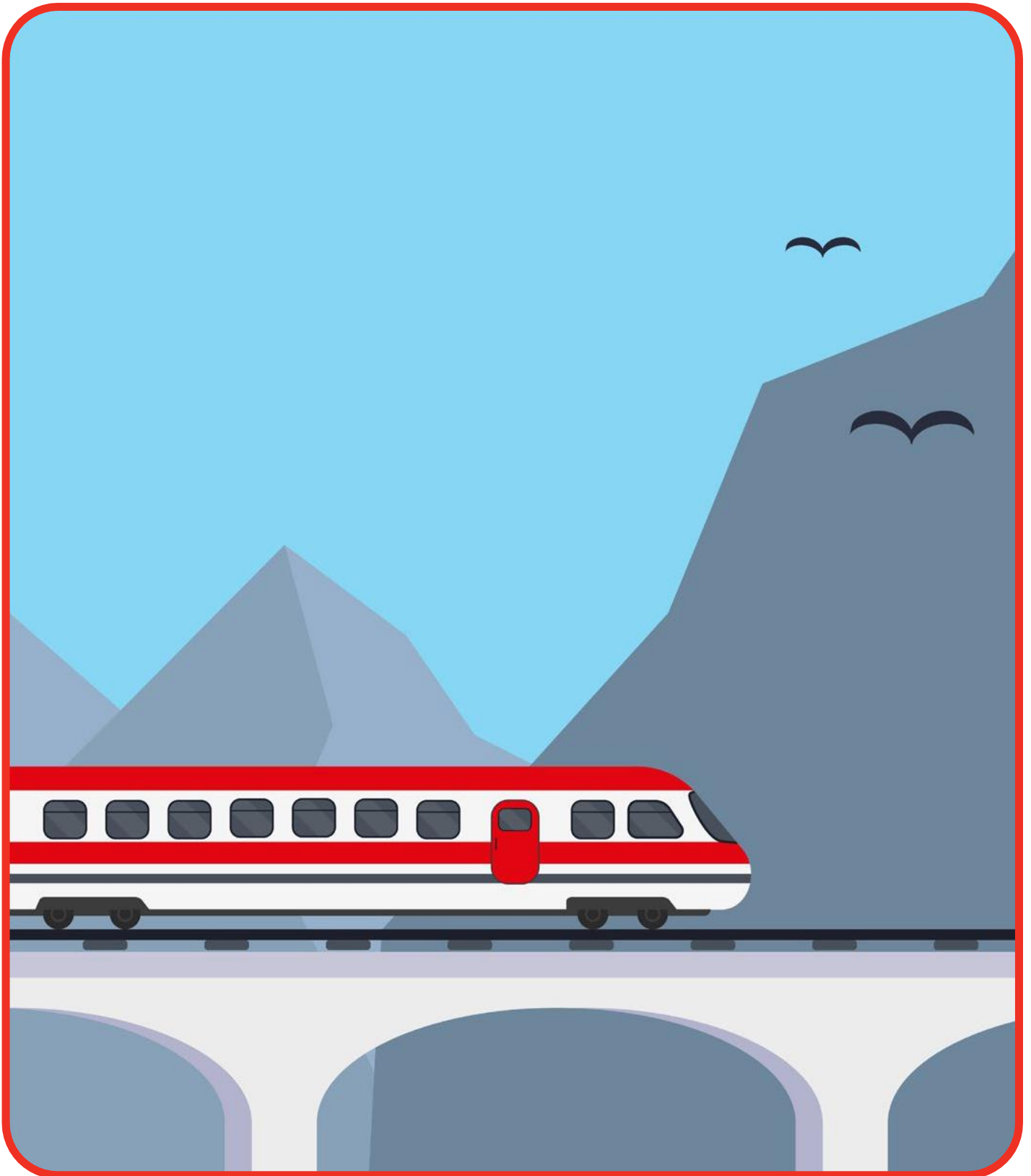
Mitglied der Geschäftsleitung IT  
Leiterin IT-Customer Journey

**Matthias Rohrbach**

Mandatsträger IT & Services

Bern, 20. Dezember 2024

## **Kapitel III:** Beschreibung des internen Kontrollsystems



## Kapitel III: Beschreibung des internen Kontrollsystems

### 3.1. Allgemeine Informationen

#### 3.1.1 Zielsetzung des Berichts

Die Transportunternehmen (TU) führen in der Regel regelmässige 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.

#### 3.1.2 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

#### 3.1.3 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. Beim relevanten Geschäftsprozess «Verkauf und Erstattung von öv-Leistungen» sind die beiden Komponenten NOVA Anbieter und NOVA Abrechnung involviert. Mögliche andere NOVA Komponenten (bsp. SwissPass oder NOVA GP) spielen keine Rolle bei diesem Geschäftsprozess und werden im Rahmen von diesem Bericht nicht weiter berücksichtigt.

**Die Vertriebskanäle** sind die Distributionswege, worüber Artikel und Angebote verkauft werden. Ein Vertriebskanal kann entweder bedient (Schalteranwendung, Chauffeurgeräte) oder unbedient (Automaten, Webshops, Mobile Applikationen) sein. Nur Transportunternehmen (z.B. SBB, Bernmobil, 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 Reporting Systeme (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 Reporting Systeme der öV-Branche (sowohl öV-Reporting als Teil des Mandats als auch als Datengrundlage für TU- bzw. verbundinterne Systeme) 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 Reporting System 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 Störfall wird aktiv die Supportorganisation aufgeboten.

**Halbtax PLUS (auch «öV-Guthaben»)** ist ein neues Produkt, welches zum 12. Dezember 2023 eingeführt wurde. Das Halbtax PLUS ist ein öV-Produkt im Sinne eines Zahlungsmittels der öV-Branche für die digitalen öV-Verkaufskanäle und somit kein Abonnement im Sinne eines Fahrausweises.

Das Halbtax PLUS besteht aus den beiden Teilen Kundeneinlage (Einzahlung des Kunden) und Bonusanteil. Bei Verwendung des Guthabens werden die Fahrausweise zu Beginn aus der Kundeneinlage bezahlt. Nachdem der Betrag der Kundeneinlage aufgebraucht ist, beginnt die Bonusphase. Ab diesem Zeitpunkt werden die Fahrausweise aus dem Bonusanteil bezahlt. Die Bonusphase endet entweder nach Ablauf eines Jahres oder nach vollständigem Aufbrauchen des Guthabens (Kundeneinlage und Bonusanteil).

Die Nutzung von Halbtax PLUS (d.h. das Ticket, das darüber gekauft wird), wird wie jeder andere Verkauf in SAP BRIM R/3 (MP3) abgebildet. Lediglich die Verträge und Guthaben von Halbtax PLUS werden im neuen SAP BRIM S/4 (MP6) System verwaltet, welches am 12. Dezember 2023 in den Produktionsbetrieb übergang. Zwischen 2025 und 2027 werden die bestehenden Services nach und nach vom bisherigen SAP BRIM (MP3) System auf das neue SAP BRIM S/4 (MP6) System transferiert.

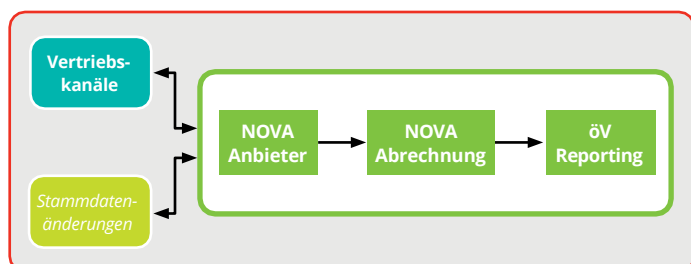
### 3.1.4 Abgrenzung innerhalb der Systemlandschaft

#### Ausklammerung und Lebensende der Prisma-Plattform

Seit den ersten Verkäufen von NOVA im Jahr 2016 wurden die beiden Verkaufsplattformen NOVA und Prisma parallel betrieben. Dabei wurde laufend das bestehende Sortiment von Prisma nach NOVA migriert. Mit der Migration des Sortiments auf NOVA wurde der Umsatz auf Prisma unbedeutend.

Die letzten wesentlichen Artikel auf Prisma wurden im Verlauf des Jahres 2023 auf NOVA migriert. Im Dezember 2023 wurde der Verkauf auf der Plattform gestoppt. Die Ablösung der Altsysteme war ein wichtiger Meilenstein in der Weiterentwicklung der Vertriebssysteme der öV-Branche.

Die Prisma-Plattform befand 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<sup>1</sup>**

PORin-Ticket war 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 im Jahr 2015 entschieden, auch den Reportingteil direkt in NOVA zu integrieren. Dafür wurde auf Basis von SAP BRIM R3 (MP3) das öV-Reporting aufgebaut.

Seit 31. Januar 2024 wurde PORin-Ticket nicht mehr beliefert und steht nur noch als «read-only» für historische Daten zur Verfügung.

## **3.2. Informationen zum funktionalen Aufbau**

### **3.2.1 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 können, wird diese Prozedur täglich rapportiert, bis die Leistung korrekt übertragen wurde.

NOVA Anbieter beliefert NOVA Abrechnung mit Daten über zwei Schnittstellen: «Leistung Notifikation» und «INTRA-Datenrelease». Leistungen (Tickets) werden in der Leistung Notifikation 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 Statistiktafel 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.

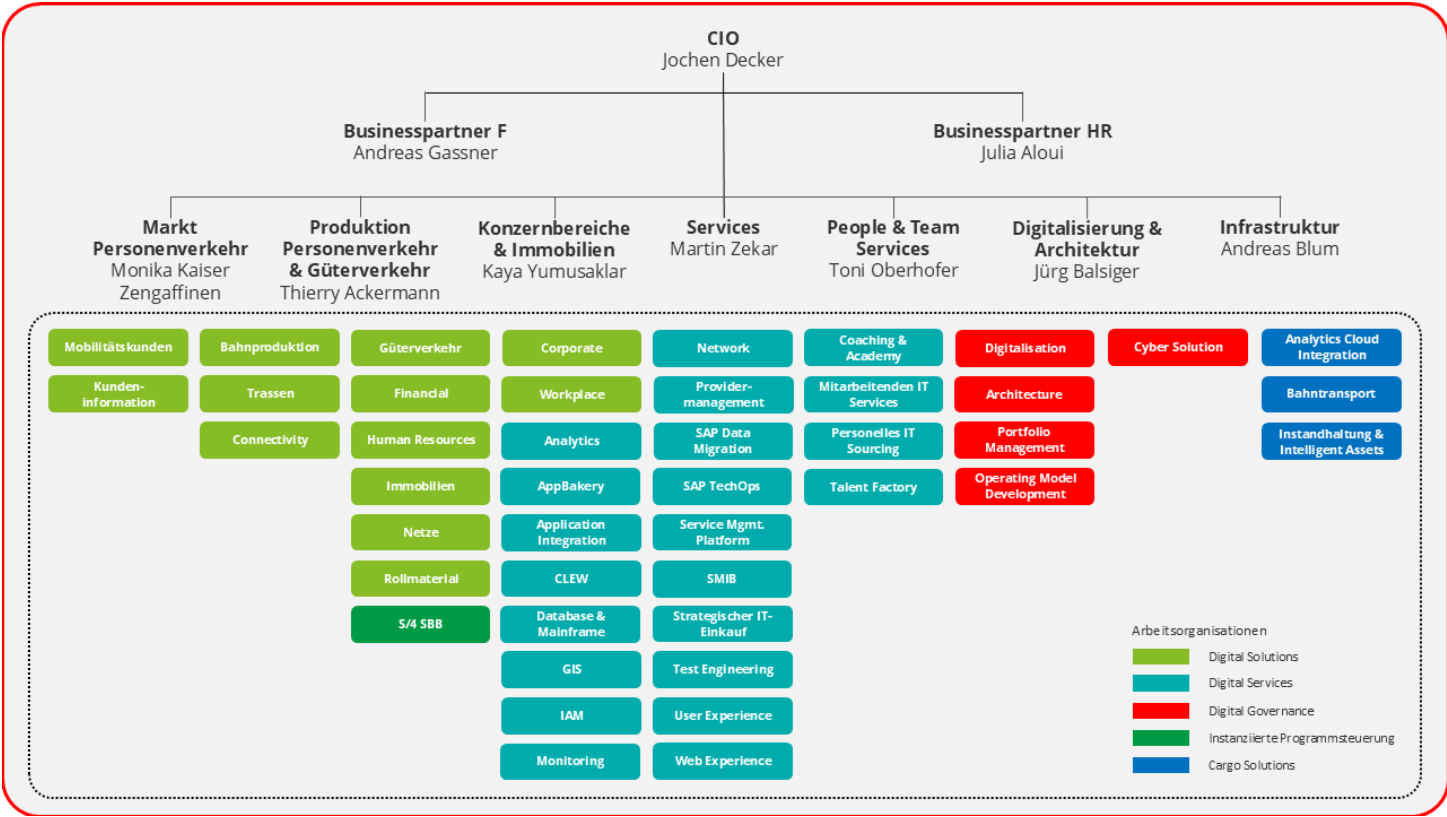
---

<sup>1</sup> PORin ist der Name des Lieferanten

3.3. Informationen zum organisatorischen Aufbau

3.3.1 Organisation und Verantwortlichkeiten

Die SBB Informatik besteht aus Digital Solutions, darunter MKS (Mobilitätskunden), und Digital Services (Stand: 30.09.2024).



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 Grégoire Ramuz (Solution Manager), Philippe Dössegger (Solution Train Engineer), Tobias Künzli und Stefan Kühnel (beide Solution Architects) und Matthias Rohrbach (Mandatsverantwortlicher IT&Services) geleitet. Für die Leistungserbringung gegenüber der öV-Branche sind die beiden Release Trains NOVA und FSS (Financial Systems & Services) relevant. Beide Agile Release Trains (NOVA ART und FSS ART) gehören zur DSO MKS.

Der NOVA ART ist für NOVA Anbieter zuständig und setzt sich aus 15 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 Detailspekte verantwortlich, wie beispielsweise das IAM (Identity and Access Management) 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.

3.4. Betriebliche Prozesse im NOVA Anbieter

3.4.1 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. Nichtsdestotrotz 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 überprüft und verifiziert.

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 Sparbilletten. 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 diese gewährten Privilegien entzieht oder den AD Account deaktiviert.

### 3.4.2 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, wird ein solcher Release detailliert überprüft und freigegeben.
- **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 erfolgen 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.

### 3.4.3 Stammdatenänderungen

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

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 des 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 die Einführung neuer Angebote, die erstmals im öV verkauft werden (seit Betriebsbeginn von NOVA wurden beispielsweise das Modul-Abo oder die Spartageskarte aufgeschaltet).
  - 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 diverse 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. Nichtsdestotrotz ist eine korrekte Angleichung der Tarifnetze an die Fahrplanänderungen wichtig, damit die betroffenen Strecken korrekt tarifiert werden.

### 3.4.4 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 Beispiele sind uneingeschränkt kombinierbar. Beispiel: Produkt: «Swiss Travel Pass Flex 3 Tage»

Anteilregel «manuell an Ausprägung»: Ausprägung Vollpreis (Person 25+), 2. Klasse:

Anteile:

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

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.

### 3.4.5 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.

### 3.5. Betriebliche Prozesse in NOVA Abrechnung & öV-Reporting

#### 3.5.1 Übersicht Finanzplattform

NOVA Abrechnung (oder öV-Abrechnung) und öV-Reporting sind Teil der Finanzplattform (vgl. untenstehende Darstellung). Die Finanzplattform ist eine auf SAP basierendes, eigenständiges Branchensystem, welche über eine 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 sämtliche 250 Transportunternehmen und 20 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 beteiligten Transportunternehmen und Verbünde abzurechnen und ein entsprechendes Finanzreporting bereitzustellen. Die Finanzplattform wird durch die ART Financial Systems & Services (FSS) im agilen Entwicklungsmodus weiterentwickelt und betrieben.

#### 3.5.2 Berechtigungsmanagement

##### SAP Access Control

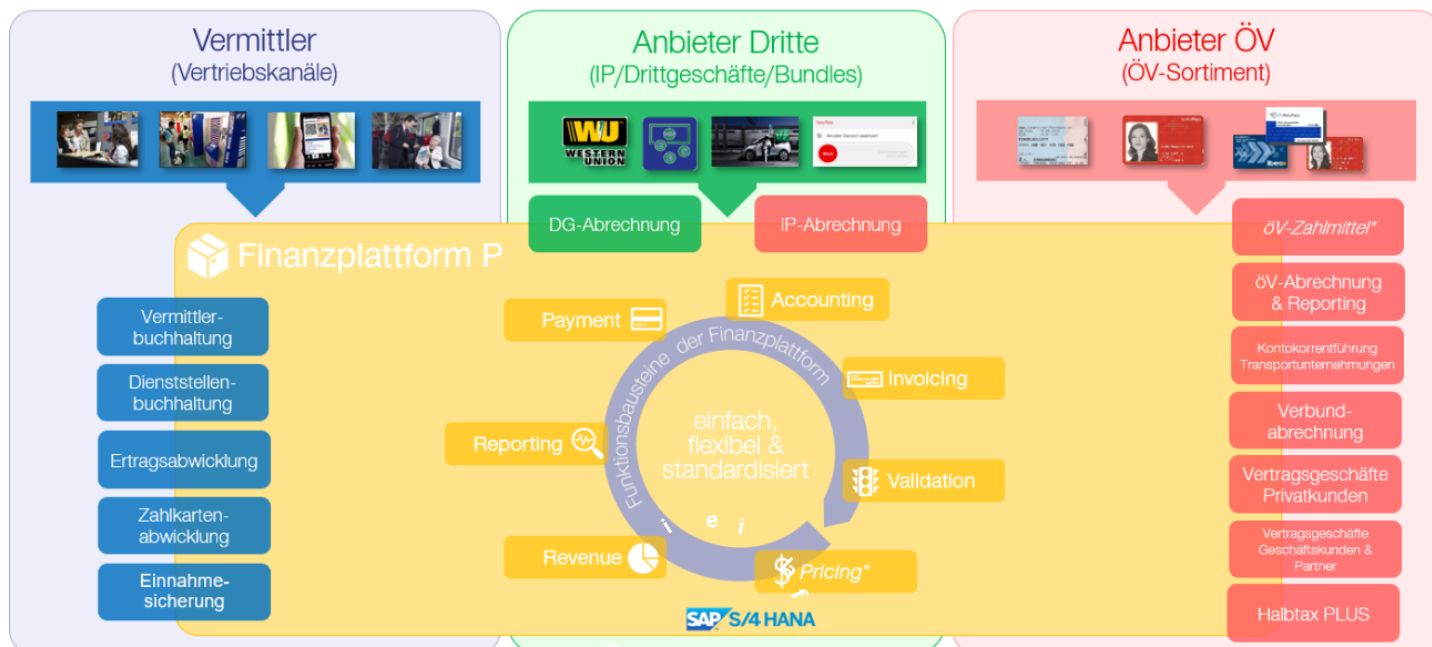
Die Finanzplattform enthält sensitive Finanz-, Unternehmens- und Personaldaten. Das Berechtigungsmanagement wird daher grundsätzlich durch den standardisierten SAP Access Control Prozess zur Verfügung gestellt und verwaltet. Im Verlauf des Jahres 2024 wird SBB-weit schrittweise von SAP GRC auf Omada als Tool für die Berechtigungsvergabe umgestellt. 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.



### 3.5.3 Change Management – NOVA Abrechnung

#### Release Planung

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

#### Beauftragung neuer Funktionalitäten

FSS setzt 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 Produkt 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 umgesetzte Teilfunktionalität mit einem Vorlauf und einer Vorabnahme bereit. FSS führt die regulären Abnahmen auf einer vorproduktiven Stufe (Integration-/ Testumgebung) mit NOVA Abrechnung durch. Bestehende Funktionalitäten werden durch automatisierte Financial Testing Framework (FIT) laufend überwacht und geprüft.

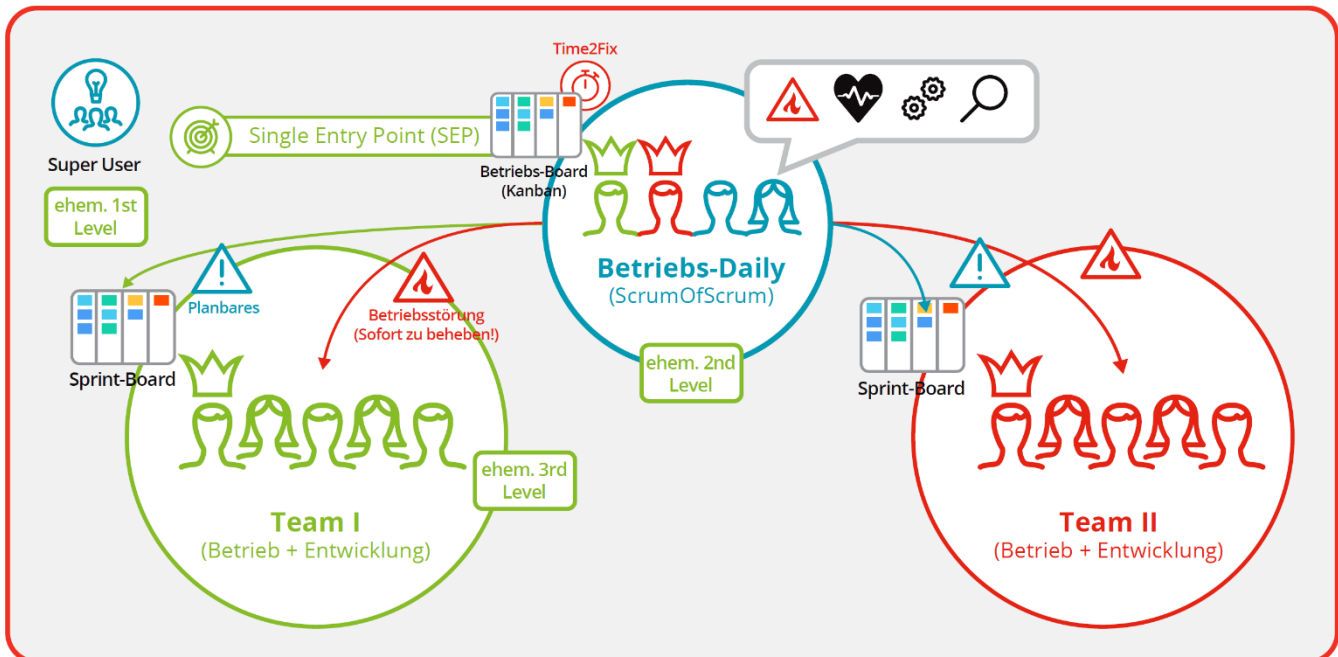
NOVA bindet die Funktionalität nachgelagert für das gemeinsame Abnahmeprüfung und der Produktivsetzung an. Die gemeinsamen Abnahmen unterliegen der Verantwortung der öV-Governance (siehe Kapitel 3.4.5).

#### 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 Triage Kriterien) behoben. Major Incidents werden ad-hoc gelöst. Defects werden im ordentlichen Release Zyklus eingeplant und behoben.

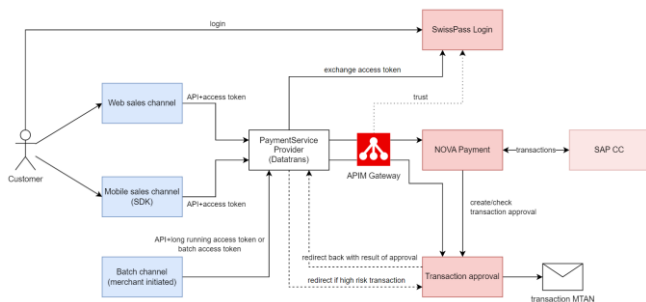
Die nachfolgende Grafik zeigt den Prozess der Fehlerbehebung inkl Triagierung:



### 3.6 Betriebliche Prozesse in Halbtax PLUS

#### 3.6.1 Übersicht Halbtax PLUS

Das Halbtax PLUS ist ein öV-Produkt im Sinne eines Zahlungsmittels der öV-Branche für die digitalen öV-Verkaufskanäle. Halbtax PLUS (HTA+) wird primär über die beiden Plattformen NOVA und SAP BRIM S/4 (MP6) abgewickelt.



Das Zahlungsmittel HTA+ auf einem Verkaufskanal funktioniert über einen Payment Service Provider, in diesem Fall Datatrans Planet, wie bei einer Kreditkarte. NOVA integriert mehrere Services (NOVA Payment, NOVA SubscriptionContract, NOVA Transaction Approval, NOVA SwissPass Token Exchange), um die Transaktionen zu begleiten. Der Swisspass Login identifiziert den Benutzer. Finanzseitig wird Halbtax PLUS auf SAP BRIM S/4 (MP6) realisiert: Halbtax PLUS ist einer von fünfzehn Services auf der Finanzplattform (vgl. Darstellung Seite 17) und stellt die Verwaltung der Kundenguthaben sicher (Verbuchung der Einzahlung, Nutzung, Erstattung, Verbuchung des Bonus).

Für die Verteilung der Bonusfinanzierung durch die öV-Branche wird gegenwärtig der bestehende Prozess der Saldierung durch den Mandatsträger Abrechnung angewandt. Es gelangt dabei bis zum 30. September 2024 in der Übergangsphase der Halbtax-Schlüssel zur Anwendung.

#### Betrieb und Weiterentwicklung

Die Finanzplattform mitsamt aller darauf laufenden 15 Services wird durch die ART Financial Systems & Services (FSS) im agilen Entwicklungsmodus weiterentwickelt und betrieben. Es werden dabei alle 15 Services gleichbehandelt.

#### 3.6.2 Berechtigungsmanagement

Da Halbtax PLUS auf den Plattformen NOVA und SAP BRIM S/4 (MP6) aufsetzen, gelten für die Berechtigungen die gleichen Voraussetzungen wie bei NOVA Anbieter (Kapitel 3.4) respektive für die NOVA Abrechnung (Kapitel 3.5.2).

#### 3.6.3 Change Management

##### Release Planung

Da Halbtax PLUS auf den Plattformen NOVA und SAP BRIM S/4 (MP6) aufsetzen, gelten für die Durchführung von Releases die gleichen Voraussetzungen wie bei NOVA Anbieter (Kapitel 3.4.2) respektive NOVA Abrechnung (3.5.3).

##### Beauftragung neuer Funktionalitäten

Da Halbtax PLUS auf den Plattformen NOVA und SAP BRIM S/4 (MP6) aufsetzen, gelten für die Beauftragung neuer Funktionalitäten die gleichen Voraussetzungen wie bei NOVA Anbieter (Kapitel 3.4.2) respektive NOVA Abrechnung (3.5.3).

##### Anforderungsmanagement

Da Halbtax PLUS auf den Plattformen NOVA und SAP BRIM S/4 (MP6) aufsetzen, gelten für das Anforderungsmanagement die gleichen Voraussetzungen wie bei NOVA Anbieter Kapitel 3.4.2) respektive NOVA Abrechnung (3.5.3).

##### Abnahme & Testing

Da Halbtax PLUS auf den Plattformen NOVA und SAP BRIM S/4 (MP6) aufsetzen, gelten für die Berechtigungen die gleichen Voraussetzungen wie bei NOVA Anbieter (Kapitel 3.4.2) respektive NOVA Abrechnung (3.5.3).

##### 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 Triage Kriterien) behoben. Major Incidents werden ad-hoc gelöst. Defects werden im ordentlichen Release Zyklus eingeplant und behoben

##### Kanalabnahme

Es wird geprüft, ob die Anbindung fachlich und Layout technisch korrekt sind. Die Abnahme ist in zwei Punkte aufgeteilt:

- Vertrag: Abschluss, Einzahlung und Kündigung
- Nutzung: Anbindung als Zahlungsmittel, Kaufe von Tickets mit Guthaben und Bonus, 2-Faktor-Authentifizierung, SAV, Ablehnung Zahlung, Sortimentseinschränkung, Befunde in Verkehrsabrechnung und korrekte Buchhaltung TU.

3.7 Kontrollen durch die Leistungsvermittler und «Nuller Prüfung»

3.7.1 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.

3.7.2 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 («Nuller Prüfung»). Allfällige Fehler werden laufend abgearbeitet und im Rahmen des Monatsabschlusses wird durch das Mandat Abrechnung der Saldo 0.00 validiert und dokumentiert.

3.7.3 Periodische Kontrollen zum Halbtax PLUS

Da es sich beim Halbtax PLUS um ein Zahlungsmittel handelt, sind einige spezifische Kontrollen eingefügt worden. Ziele der Kontrollen sind:

- Die korrekte Zuordnung von Vertrag und Kundenkonto sicherzustellen
- Die korrekte Abrechnung aller bezogenen Leistungen sicherzustellen (inkl. Sperrung bei Diebstahl / Verlust)
- Diebstahl und missbräuchliche Auszahlungsbegehren von Guthaben zu verhindern
- Die Vorgaben der FINMA bzgl. der Einhaltung der Guthabenslimiten einzuhalten
- Die Belastung der TU bei der Finanzierung des Bonus gemäss freigegebenem Schlüssel abzuwickeln.

Der zugrundeliegende Verteilschlüssel (für die Periode Dezember 2023 (Go Live Halbtax PLUS) bis September 2024 basiert auf dem Entscheid den Halbtax Verteilschlüssel zu verwenden. Dieser wird durch die Geschäftsstelle der Alliance SwissPass zur Verfügung gestellt und dessen Herleitung somit nicht Bestandteil dieses Berichtes.

3.8 Ergänzende übergreifende Kontrollen

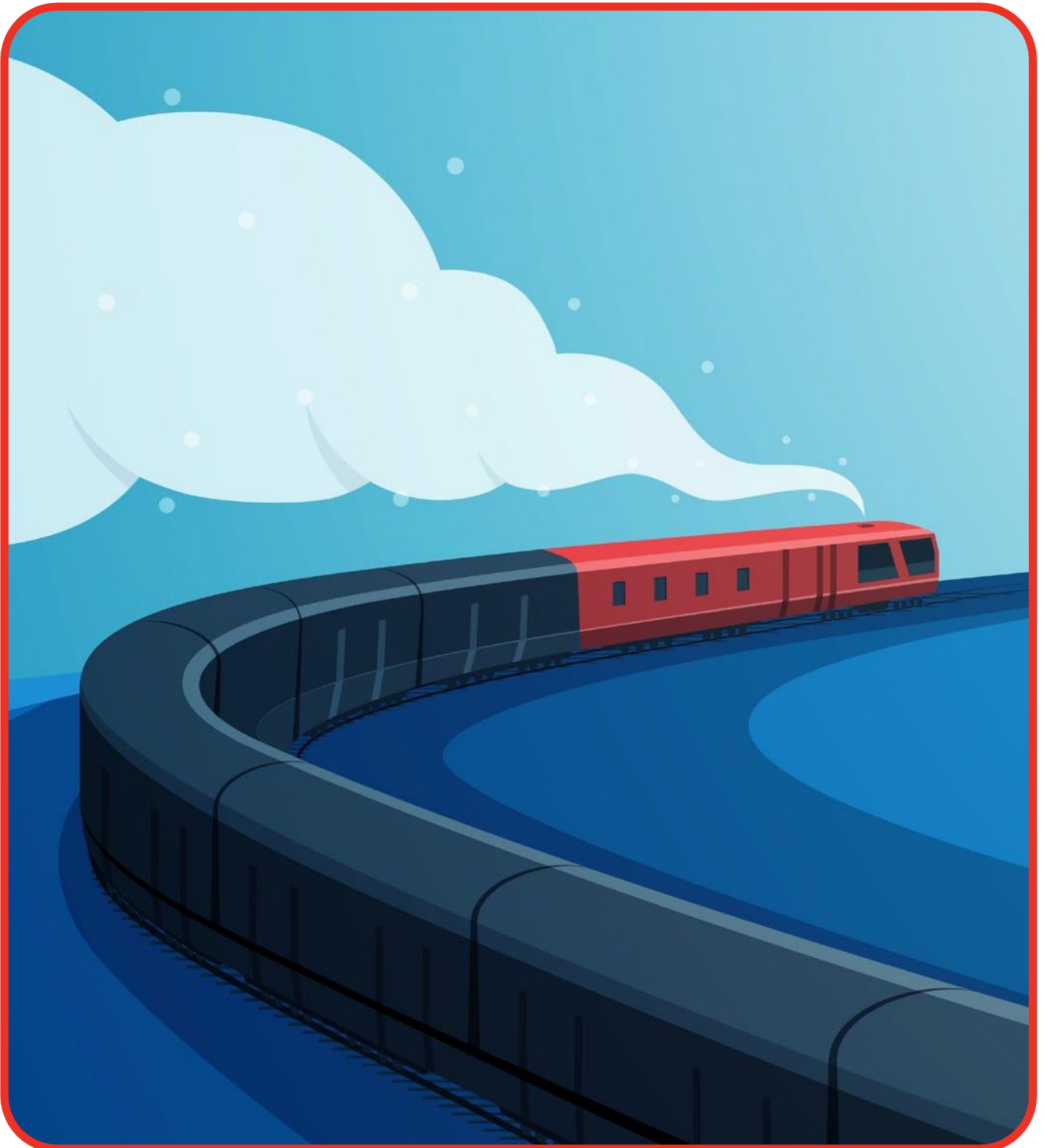
3.8.1 Ergänzende Benutzerentitätskontrollen

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:

|                   |                                                                                                                                                                                                       |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 Zugriffsänderungen der SBB, damit diese umgesetzt werden können.                                                                                                     |

Alle auf SAP BRIM aufsetzenden Zugriffsrechte werden standardisiert über SAP GRC bzw. Omada beantragt, verwaltet und bei Bedarf entzogen. Neue Berechtigungen werden im 4-Augen-Prinzip geprüft und freigegeben. Die Kombination von kritischen Berechtigungen werden durch eine Risikoanalyse in SAP GRC bzw. Omada angezeigt und erfordern eine gesonderte Freigabe. Es findet jährlich ein Review der erteilten Berechtigungen durch den Rolleninhaber statt.

## **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 Zugriffssicherheit 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 zeitnah angepasst wird sowie die hochprivilegierten Accounts angemessen vergeben sind.

| Kontroll-ID | Kontrollbeschreibung                                                                                                                                                                                                                                                                                                                   | Prüfungshandlung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Resultat                       |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| 1.1         | <b>Zugriffsberechtigung</b><br><br>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.<br><br>Stichprobenbasierte Prüfung von vergebenen NOVA Anbieter Berechtigungen, um sicherzustellen, dass die Berechtigungen angefragt und von den Fachverantwortlichen genehmigt werden.                                                                                                                                                                                                                                                                                                                          | Keine Abweichung festgestellt. |
| 1.2         | <b>Zugriffsentzug</b><br><br>Ausgetretenen SBB-Mitarbeitenden wird der AD-Zugriff zeitnah entzogen.<br><br>Die Gültigkeit der AD-Benutzer der Mitarbeitenden, die nicht für die SBB arbeiten, ist auf maximal 500 Tage beschränkt. Bei der Bestellung des Benutzers per Formular kann die Gültigkeit nicht mehr als 500 Tage betragen. | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br><br>Stichprobenbasierte Prüfung von SBB-internen Austritten, um sicherzustellen, dass diese rechtzeitig von den Fachverantwortlichen der zuständigen Stelle mitgeteilt und deren Zugriffe entfernt werden.<br><br>Inspektion des Bestellprozesses für externe Benutzer, um sicherzustellen, dass eine Bestellung mit einer Gültigkeit von mehr als 500 Tagen nicht möglich ist.<br><br>Stichprobenbasierte Prüfung von externen Benutzern, um festzustellen, dass diese nicht länger als 500 Tage gültig sind. | Keine Abweichung festgestellt. |
| 1.3         | <b>Überprüfung der Benutzerzugriffsrechte</b><br><br>Die kritischen Zugriffsberechtigungen werden jährlich überprüft.                                                                                                                                                                                                                  | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br><br>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.<br><br>Inspektion der jährlichen Rezertifizierung, um sicherzustellen, dass der kritische Systemzugriff rechtzeitig und in angemessener Weise geändert wird.                                                       | Keine Abweichung festgestellt. |

| Kontroll-ID | Kontrollbeschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Prüfungshandlung                                                                                                                                                                                                                                                                                                                                         | Resultat                       |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| 1.4         | <b>Authentifizierung</b><br><br>Die Authentifizierung für den Zugriff auf NOVA Anbieter erfolgt per AD. Passworteinstellungen stellen sicher, dass der Zugang geschützt ist. Die Passwortparameter entsprechen mindestens den folgenden Kriterien: <ul style="list-style-type: none"> <li>• Passwortlänge: 12</li> <li>• Passwortkomplexität: aktiviert</li> <li>• Passwortablaufdatum: 90 Tage ausser dauerhaftem und sicherem Passwort</li> <li>• Passworthistorie: 18</li> <li>• Fehlerhafte Versuche: 5</li> </ul> | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br><br>Inspektion der Default Domain Policy und Beurteilung, ob die Parameter gemäss den internen Passwortrichtlinien eingestellt sind.                                                                                                | Keine Abweichung festgestellt. |
| 1.5         | <b>Privilegierter Zugriff</b><br><br>Der Zugriff auf kritische Rollen ist autorisiert und entsprechend eingeschränkt.                                                                                                                                                                                                                                                                                                                                                                                                  | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br><br>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 Abweichung 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         | <b>Zugriffsberechtigung</b><br><br>Art und Umfang der Benutzerzugriffsrechte für neue und geänderte Benutzerzugriffe werden genehmigt.                                                                           | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br><br>Stichprobenbasierte Prüfung von vergebenen SAP Berechtigungen, um sicherzustellen, dass diese per Antrag angefragt und von den Fachverantwortlichen genehmigt wird.                                                                                                                                                                                                                                                                  | Keine Abweichung festgestellt.                                                                                                                                                                                                                                                                     |
| 2.2         | <b>Zugriffsentzug</b><br><br>Ausgetretenen SBB-Mitarbeitenden wird der Zugriff auf SAP zeitnah entzogen.<br><br>Die Gültigkeit der SAP-Benutzer der externen Mitarbeitenden ist auf maximal 500 Tage beschränkt. | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br><br>Kritische Durchsicht des Austrittsprozesses, um sicherzustellen, dass dieser dokumentiert ist.<br><br>Stichprobenbasierte Prüfung von SBB internen Austritten, um sicherzustellen, dass diese rechtzeitig von den Fachverantwortlichen der zuständigen Stelle mitgeteilt und deren Zugriff entfernt wird.<br><br>Stichprobenbasierte Prüfung von externen Benutzern, um sicherzustellen, dass Zugriffe auf 500 Tage beschränkt sind. | Wir haben festgestellt, dass 15 externe Mitarbeitende im SAP-System von NOVA Abrechnung entgegen den Reglementen der SBB mehr als 500 Tage gültig waren.<br><br>Die 15 externen Mitarbeitenden sind alle in der kurz zuvor durchgeführten Überprüfung der Benutzerzugriffsrechte bestätigt wurden. |

| Kontroll-ID | Kontrollbeschreibung                                                                                                                                                                                                                                                                                                                                                                                                                       | Prüfungshandlung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Resultat                                                                                                                                                                                                                                                                                                                                      |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.3         | <b>Überprüfung der Benutzerzugriffsrechte</b><br>Die kritischen Zugriffsberechtigungen werden regelmässig überprüft.                                                                                                                                                                                                                                                                                                                       | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br>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.<br>Inspektion der jährlichen Rezertifizierung, um sicherzustellen, dass der kritische Systemzugriff rechtzeitig und in angemessener Weise geändert wird. | Wir haben eine Stichprobe von Berechtigungen geprüft, die während der Rezertifizierung von Rolleninhabern als unangemessen identifiziert wurden. Dabei haben wir festgestellt, dass in 5 von 25 Fällen die unangemessenen Berechtigungen erst nach ungefähr 30 Tagen entzogen wurden, wodurch der Berechtigungsentzug nicht zeitnah erfolgte. |
| 2.4         | <b>Authentifizierung</b><br>Passwordeinstellungen stellen sicher, dass der Zugang geschützt ist. Die Passwortparameter entsprechen mindestens den folgenden Kriterien: <ul style="list-style-type: none"> <li>• Passwortlänge: 12</li> <li>• Passwortkomplexität: aktiviert</li> <li>• Passwortablaufdatum: 90 Tage ausser dauerhaftem und sicherem Passwort</li> <li>• Passworthistorie: 18</li> <li>• Fehlerhafte Versuche: 5</li> </ul> | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br>Inspektion der SAP-Passwortparameter, um sicherzustellen, dass die Parameter gemäss den internen Passwortrichtlinien eingestellt sind.<br>Inspektion der Default Domain Policy und Beurteilung, ob die Passwort Parameter gemäss den internen Passwortrichtlinien eingestellt sind., um sicherzustellen, dass diese angemessen sind.                                                                                                            | Keine Abweichung festgestellt.                                                                                                                                                                                                                                                                                                                |
| 2.5         | <b>Privilegierter Zugriff</b><br>Der Zugriff auf kritische Berechtigungen ist autorisiert und entsprechend eingeschränkt.                                                                                                                                                                                                                                                                                                                  | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br>Inspektion von kritischen Berechtigungen von SAP-Benutzern, um sicherzustellen, dass diese angemessen eingeschränkt sind.                                                                                                                                                                                                                                                                                                                       | Keine Abweichung festgestellt.                                                                                                                                                                                                                                                                                                                |
| 2.6         | <b>Zugriffskonfiguration</b><br>Die Passwörter der Standard-SAP-Benutzer wurden geändert und werden sicher verwahrt.                                                                                                                                                                                                                                                                                                                       | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br>Inspektion der Standardpasswörter für Standard-SAP-Benutzern, um sicherzustellen, dass diese in allen Mandanten geändert und entsprechend gesichert sind.                                                                                                                                                                                                                                                                                       | Keine Abweichung festgestellt.                                                                                                                                                                                                                                                                                                                |

| Kontroll-ID | Kontrollbeschreibung                                                                                                                                                                                                          | Prüfungshandlung                                                                                                                                                                                                                                                                                                                                                                                                                                               | Resultat                                                                                                                                                                                                                                                                                                                                                                   |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.7         | <p><b>SAP_ALL und SAP_NEW</b></p> <p>Dialog und Service Benutzern sind keine SAP_ALL oder SAP_NEW Profile dauerhaft zugeordnet.</p> <p>Temporärer SAP_ALL/ SAP_NEW Zugang wird angefragt, genehmigt und zeitnah entzogen.</p> | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion aller dauerhaft vergebenen SAP_ALL und SAP_NEW Profilen, um sicherzustellen, dass diese keinen Dialog und Service Benutzern dauerhaft zugeordnet sind.</p> <p>Inspektion aller temporär zugeordneten SAP_ALL und SAP_NEW Profilen, um sicherzustellen, dass diese angefragt, genehmigt und zeitnah entzogen werden.</p> | <p>Wir haben festgestellt, dass ein Benutzer das hochprivilegierte Profil SAP_ALL zugewiesen war, welches die Ausführung aller Transaktionen in NOVA Abrechnung ermöglicht und gemäss SBB-Richtlinien nur kurzfristig und bei aktuellem Bedarf vergeben werden darf. Im Rahmen unserer Prüfung haben wir jedoch festgestellt, dass der Benutzer nicht verwendet wurde.</p> |
| 2.8         | <p><b>Notfallberechtigungen</b></p> <p>Die Benutzung von Notfallberechtigungen werden protokolliert und bis spätestens am 15. Tag des Folgemonats überprüft.</p>                                                              | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion des Notfallbenutzer-Prozesses, um sicherzustellen, dass alle Benutzungen protokolliert werden.</p> <p>Inspektion aller Benutzungen von Notfallberechtigungen, um festzustellen, dass diese zeitnah überprüft werden.</p>                                                                                                | <p>Bei der Prüfung der Reviews von Notfallberechtigungs-Protokollen haben wir festgestellt, dass 19 Protokolle nicht zeitnah überprüft wurden.</p>                                                                                                                                                                                                                         |

#### 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         | <b>Aufgabentrennung</b><br>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.<br><br>Stichprobenbasierte Prüfung von Änderungen, um sicherzustellen, dass die Fachprüfung durch eine andere Person als den Entwicklern durchgeführt wird.                                              | Keine Abweichung festgestellt. |
| 3.2         | <b>Testen und Freigabe</b><br>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.<br><br>Stichprobenbasierte Prüfung von Änderungen, um festzustellen, ob die Major Releases durch den Release Manager freigegeben werden und es keine verhindernden Mängel vor der Produktivsetzung gibt. | Keine Abweichung festgestellt. |
| 3.3         | <b>Fachprüfungen durchgeführt</b><br>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.<br><br>Stichprobenbasierte Prüfung von Änderungen, um sicherzustellen, dass für alle Software-Versionsänderungen von NOVA Anbieter Fachprüfungen vorgenommen werden.                                     | Keine Abweichung festgestellt. |
| 3.4         | <b>Systemlandschaften</b><br>Es existiert eine getrennte Entwicklungs-, Integrations- sowie Produktionsumgebung für NOVA Anbieter.                                                          | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br><br>Inspektion der Systemlandschaft, um sicherzustellen, dass es eine getrennte Entwicklungs-, Integrations- sowie Produktionsumgebung gibt.                                                          | Keine Abweichung 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         | <b>Testen von Änderungen</b><br><br>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.<br><br>Stichprobenbasierte Prüfung von SAP-Transporten, um sicherzustellen, dass diese vor der Produktivsetzung getestet und genehmigt werden.                           | Keine Abweichung festgestellt. |
| 4.2         | <b>Systemlandschaften</b><br><br>Es existiert eine getrennte Entwicklungs-, Test- sowie Produktionsumgebung für NOVA Abrechnung.                                    | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br><br>Inspektion der Systemlandschaft, um sicherzustellen, dass eine getrennte Entwicklungs-, Test- sowie Produktionsumgebung existiert.                                | Keine Abweichung festgestellt. |
| 4.3         | <b>Berechtigungen Mandats-/ Systemöffnungen</b><br>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.<br><br>Inspektion aller SAP-Benutzer, die System- oder Mandantenöffnungen vornehmen können, um sicherzustellen, dass diese angemessen eingeschränkt sind.                | Keine Abweichung festgestellt. |
| 4.4         | <b>System- und Mandantenöffnungen</b><br><br>System- und Mandantenöffnungen sind auf ein Minimum beschränkt und werden zuvor genehmigt.                             | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br><br>Inspektion aller System- und Mandantenöffnungen, um sicherzustellen, dass diese angemessen und genehmigt sind.                                                    | Keine Abweichung festgestellt. |
| 4.5         | <b>Transportberechtigungen</b><br><br>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.<br><br>Inspektion aller SAP-Benutzer, die die Berechnung haben, Änderungen in die Produktion einzuspielen, um sicherzustellen, dass diese angemessen eingeschränkt sind. | Keine Abweichung festgestellt. |

| Kontroll-ID | Kontrollbeschreibung                                                                          | Prüfungshandlung                                                                                                                                                                                                                                    | Resultat                       |
|-------------|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| 4.6         | <b>Debug Berechtigungen</b><br>Debug Zugriff wird nicht dauerhaft in der Produktion vergeben. | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br>Inspektion aller SAP-Benutzer, die Debug Berechtigungen haben, um sicherzustellen, dass diese nicht dauerhaft vergeben werden. | Keine Abweichung 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         | <b>4-Augenprinzip bei wöchentlichen Datenrelease</b><br><br>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.<br><br>Stichprobenbasierte Prüfung von neuen Produkten, um sicherzustellen, dass die Fachprüfung durch eine andere Person durchgeführt wird als die Anpassung der finanzrelevanten Stammdaten.<br><br>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 Abweichung festgestellt. |
| 5.2         | <b>4-Augen-Prinzip bei Mutationen zum Datenstandwechsel</b><br><br>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.<br><br>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.<br><br>Stichprobenbasierte Prüfung der internen Kontrolle, um sicherzustellen, dass Änderungen im 4-Augen-Prinzip durchgeführt werden.                                                     | Keine Abweichung festgestellt. |
| 5.3         | <b>Datenmutationsprüfung</b><br><br>Das Datenmanagement-Team prüft die korrekte Umsetzung einer Stichprobe von 30 Mutationen pro Quartal an Streckensperrungen, Tarifnetz-Relationentarifmodell sowie im Tarifnetz-Verbundnetz.<br><br>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.<br><br>Stichprobenbasierte Prüfung der internen Kontrolle, um sicherzustellen, dass diese durchgeführt wird und die überprüften Streckensperrungen, Tarifnetz-Relationentarifmodell sowie Preisberechnung korrekt durchgeführt wurden.                                                                                                                                                                               | Keine Abweichung festgestellt. |

| Kontroll-ID | Kontrollbeschreibung                                                                                                                                                                                                                                | Prüfungshandlung                                                                                                                                                                                                                                                                                                                                                   | Resultat                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| 5.4         | <b>Anteils- und Preisberechnung</b><br><br>Anteils- und Preisberechnung aller neuen Produkte werden überprüft, um festzustellen, ob diese korrekt berechnet werden.                                                                                 | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br><br>Stichprobenbasierte Prüfung von neuen Produkten (Zonen, Fixpreis, DV), um sicherzustellen, dass die Anteils- und Preisberechnung gemäss der Bestellung implementiert werden.                                                              | Keine Abweichung festgestellt. |
| 5.5         | <b>Vertriebskonfigurationsänderung</b><br><br>Die Verkaufs- und Zahlungslogs der Transaktionen nach einer Vertriebskonfigurationsänderung (Produkt, Kanal) sind korrekt und die Dienststellenbuchhaltung wird in den entsprechenden Konten gebucht. | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br><br>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 Abweichung 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         | <p><b>Einlieferung zu NOVA Abrechnung</b></p> <p>Die Übertragung aller Leistungen von NOVA Anbieter an NOVA Abrechnung wird täglich und automatisch geprüft.</p> <p>Sollte eine Leistung nicht übertragen werden, wird dieser Fehler täglich wieder rapportiert, bis die Leistung korrekt übertragen wird. Das NOVA Partnermanagement-Team stellt sicher, dass der Fehler korrigiert und alle Leistungen übertragen werden.</p> | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion der Schnittstelle, um sicherzustellen, dass diese überwacht wird und keine unbegründeten Fehler beinhaltet.</p> <p>Inspektion der Arbeitsanweisung, um sicherzustellen, dass diese die Überwachung der Schnittstelle beinhaltet.</p>             | Keine Abweichung festgestellt. |
| 6.2         | <p><b>Befüllung der öV-Reporting</b></p> <p>Die Befüllung aller Leistungen innerhalb NOVA Abrechnung/öV-Reporting wird täglich und automatisch in Streamworks geprüft.</p> <p>Abbrüche werden zeitnah bearbeitet, Fehler korrigiert und Übertragungen neu gestartet.</p>                                                                                                                                                        | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion der Streamworks Jobs, um sicherzustellen, dass sie täglich ausgeführt werden.</p> <p>Inspektion einer Stichprobe von Abbrüchen, um sicherzustellen, dass diese zeitnah bearbeitet, Fehler korrigiert und Übertragungen neu gestartet werden.</p> | Keine Abweichung festgestellt. |
| 6.3         | <p><b>Vollständige Verteilung der Verkäufe</b></p> <p>Ein Abstimmbericht «Nuller Prüfung» 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.</p>                     | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion des Abstimmungsberichtes «Nuller Prüfung», 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.</p>           | Keine Abweichung festgestellt. |

| Kontroll-ID | Kontrollbeschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Prüfungshandlung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Resultat                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| 6.4         | <p><b>Authentifizierung</b> Die Authentifizierung für den Zugriff auf Streamworks erfolgt per AD. Passworteinstellungen oder lokalen Authentifizierung (Technische Benutzer) und stellen sicher, dass der Zugang geschützt ist.</p> <p>Die Passwortparameter entsprechen mindestens den folgenden Kriterien: Passwortlänge:</p> <ul style="list-style-type: none"> <li>• Passwortlänge: 12</li> <li>• Passwortkomplexität: aktiviert</li> <li>• Passwortablaufdatum: 90 Tage ausser dauerhaftem und sicherem Passwort</li> <li>• Passworthistorie: 18</li> <li>• Fehlerhafte Versuche: 5</li> </ul> | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion der Default Domain Policy und Beurteilung, ob die Parameter gemäss den internen Passwortrichtlinien eingestellt sind.</p> <p>Inspektion der lokalen Passworteinstellung und Beurteilung, ob die Parameter gemäss den internen Passwortrichtlinien eingestellt sind sofern technisch möglich.</p> <p>Stichprobenbasierte Prüfung von Benutzern, ob diese der korrekten Authentifizierungsmethode zugeordnet sind.</p> | Keine Abweichung festgestellt. |
| 6.5         | <p><b>Privilegiertes Zugriff</b></p> <p>Der Zugriff auf kritische Berechtigungen ist autorisiert und entsprechend eingeschränkt.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion von kritischen Berechtigungen von Streamworks-Benutzern, um sicherzustellen, dass diese angemessen eingeschränkt sind.</p>                                                                                                                                                                                                                                                                                           | Keine Abweichung festgestellt. |
| 6.6         | <p><b>Zugriff auf Stream-Planung</b></p> <p>Der Zugriff auf nicht eigene Streams sowie deren Einplanung zu modifizieren ist autorisiert und entsprechend eingeschränkt.</p>                                                                                                                                                                                                                                                                                                                                                                                                                         | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion von Stream Berechtigungen von Streamworks-Benutzern, um sicherzustellen, dass diese angemessen eingeschränkt sind.</p>                                                                                                                                                                                                                                                                                               | Keine Abweichung festgestellt. |
| 6.7         | <p><b>Streamwork Monitoring</b></p> <p>In Streamworks wird der erfolgreiche Abschluss der Streams überwacht und fehlgeschlagene Streams werden bei Bedarf erneut durchgeführt.</p>                                                                                                                                                                                                                                                                                                                                                                                                                  | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion des Streamworks Monitoring Dashboards, um sicherzustellen, dass der erfolgreiche Abschluss hin überwacht werden, und fehlgeschlagene Streams bei Bedarf erneut gestartet werden.</p> <p>Inspektion aller relevanten Streams, um sicherzustellen, dass die Stream-Verantwortlichen über einen Stream Abbruch informiert werden.</p>                                                                                   | Keine Abweichung festgestellt. |

## 4.7 Halbtax PLUS

**Kontrollziel 7** – Die Kontrollen stellen angemessen sicher, dass das Guthaben und der Bonus von Halbtax PLUS vollständig abgerechnet wird.

| Kontroll-ID | Kontrollbeschreibung                                                                                                                                                                                                                                                                                                                                                            | Prüfungshandlung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Resultat                       |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| 7.1         | <p><b>Guthaben wird bei Nutzung nicht vermindert</b></p> <p>Die Übertragung aller Leistungen mit dem Zahlungsmittel Halbtax PLUS an NOVA Abrechnung wird täglich geprüft.</p> <p>Wird eine Leistung nicht belastet, stellt das Team Betrieb Finanzplattform aus dem Mandat Abrechnung die Korrektur sicher.</p>                                                                 | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion des Abstimmungsberichtes, um sicherzustellen, dass allfällige Fehler laufend abgearbeitet wurden und im durch das Mandat Abrechnung validiert und dokumentiert wurde.</p> <p>Inspektion einer Stichprobe von Korrekturen, um sicherzustellen, dass diese zeitnah bearbeitet und die Korrekturen nachvollziehbar dokumentiert wurden.</p>                  | Keine Abweichung festgestellt. |
| 7.2         | <p><b>Datenverlust durch Unterbrüche, Störungen</b></p> <p>Nach Unterbrüchen und Störungen werden die Logs der einzelnen NOVA Abrechnung-Komponenten abgeglichen und wo notwendig durch die ART FSS bis zum Datengleichstand neu synchronisiert.</p> <p>Durch tägliche Synchronisierungsjobs zwischen NOVA Abrechnungs-Komponenten werden fehlende Elemente synchronisiert.</p> | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion einer Stichprobe von Unterbrüchen und Störungen, um sicherzustellen, dass diese zeitnah bearbeitet und Massnahmen nachvollziehbar dokumentiert wurden.</p> <p>Inspektion des Monitoring Dashboards, um sicherzustellen, dass Synchronisierungsjob überwacht werden und fehlgeschlagene Jobs bei Bedarf erneut gestartet werden.</p>                       | Keine Abweichung festgestellt. |
| 7.3         | <p><b>Korrekte Pflege des Halbtax PLUS Schlüssels</b></p> <p>Der im System verwendete Halbtax PLUS Schlüssel wird gemäss den Vorgaben der Alliance Swiss Pass durch das Pflgeteam bei NOVA eingepflegt.</p>                                                                                                                                                                     | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion im System, um festzustellen, ob der Halbtax PLUS Schlüssel gemäss den Vorgaben im System eingepflegt ist.</p>                                                                                                                                                                                                                                             | Keine Abweichung festgestellt. |
| 7.4         | <p><b>Falsche Verteilung der Bonusfinanzierung an die TU</b></p> <p>Durch die Anwendung des korrekten Verteilschlüssels ist sichergestellt, dass alle TU bei der Verteilung der Bonusfinanzierung den berechneten Anteil erhalten.</p> <p>Die Bonusverteilung inklusive Korrekturen werden im 4-Augen-Prinzip durchgeführt.</p>                                                 | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion im System, ob alle Transportunternehmen dem Halbtax PLUS Schlüssel zugewiesen sind und somit bei der Verteilung der Bonusfinanzierung den berechneten Anteil erhalten.</p> <p>Inspektion der Änderungshistorien, um sicherzustellen, dass die initiale Zuweisung des Halbtax PLUS Schlüssels sowie Änderungen im 4-Augen-Prinzip durchgeführt wurden.</p> | Keine Abweichung festgestellt. |

|     |                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                |
|-----|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| 7.5 | <b>Unvollständig abgerechnete Bonusanteile</b> | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>Inspektion des Abstimmungsberichtes zur Belastung aller TUs, um sicherzustellen, dass alle abgerechneten Bonusanteile vollständig an die TU verteilt wurden, allfällige Fehler laufend abgearbeitet wurden und im Rahmen des Monatsabschlusses durch das Mandat Abrechnung der Saldo 0.00 validiert und dokumentiert wurde.</p> | Keine Abweichung festgestellt. |
|     |                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                |

#### 4.8 Backup

**Kontrollziel 8** – Die Kontrollen stellen angemessen sicher, dass NOVA Abrechnung nach einem Katastrophenfall wieder erstellt werden kann.

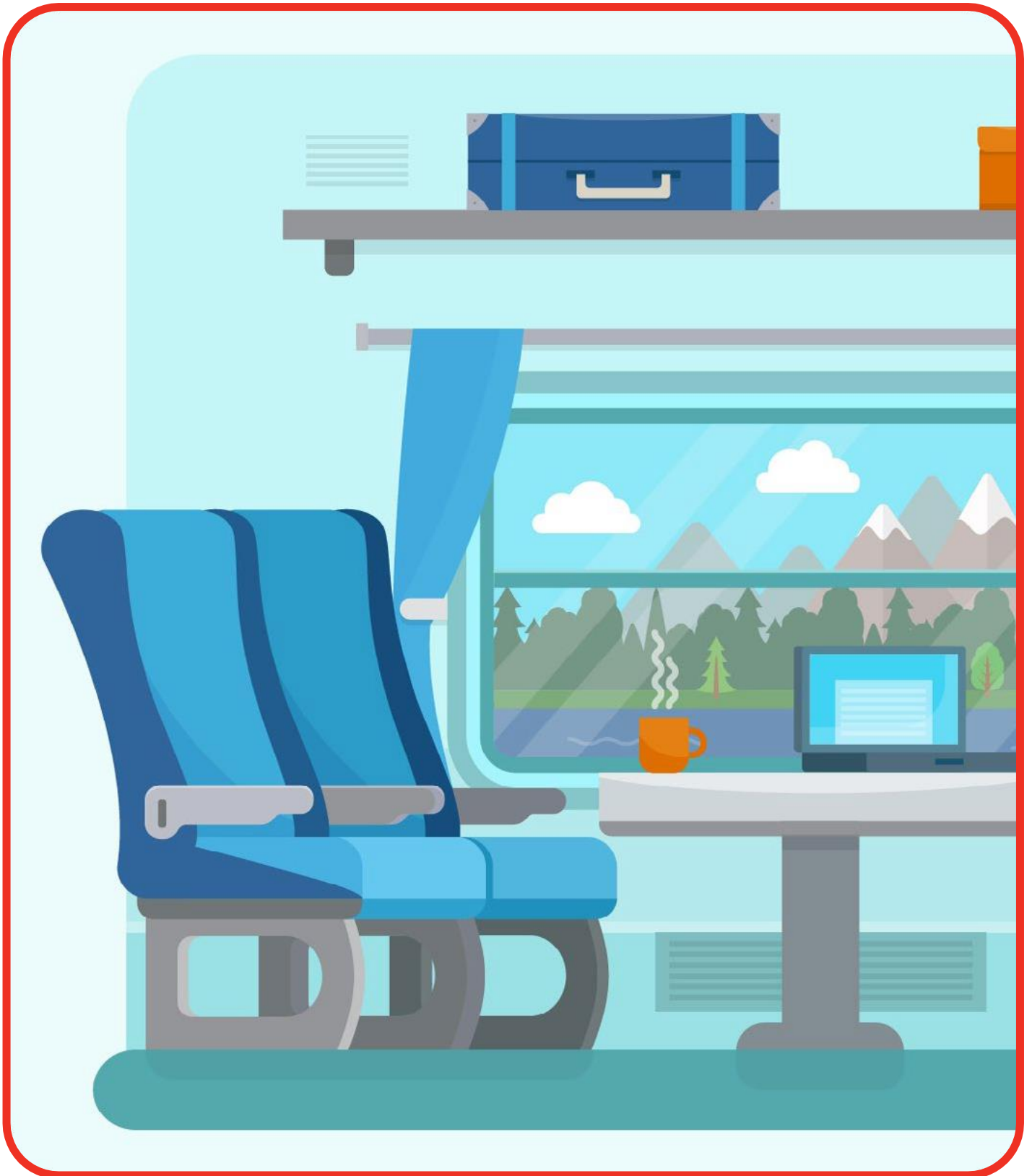
| Kontroll-ID | Kontrollbeschreibung                                                                                                                                                                                                                                     | Prüfungshandlung                                                                                                                                                                                                                                                                                                                                                                                | Resultat                       |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| 8.1         | <b>Erstellung von Backups</b><br><br>Die Finanzdaten werden nach einem festgelegten Zeitplan in regelmässigen Abständen gesichert.                                                                                                                       | Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.<br><br>Inspektion der Backup-Konfigurationen, um sicherzustellen, dass die Backups auf den Servern gemäss den SBB-Richtlinien angestossen werden.                                                                                                                             | Keine Abweichung festgestellt. |
| 8.2         | <b>Backup Monitoring</b><br><br>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.<br><br>Inspektion der Backup-Prozesse, um sicherzustellen, dass die Ausführung überwacht, wird und relevante Fehler eskaliert werden.<br><br>Inspektion eines Restore-Tests, um sicherzustellen, dass ein solcher während dem Berichtszeitraum erfolgreich durchgeführt wird. | Keine Abweichung festgestellt. |

#### 4.9 ISAE-Berichte von Dienstleistern

**Kontrollziel 9** – 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                       |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| 9.1         | 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. | <p>Befragung des Kontrollverantwortlichen, um sicherzustellen, dass die Kontrolle wie beschrieben durchgeführt wird.</p> <p>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.</p> | Keine Abweichung 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 dienstleistungsbezogenen internen Kontrollsystems durch SBB. Die in Kapitel V enthaltenen Informationen wurden nicht bei der Prüfung des dienstleistungsbezogenen internen Kontrollsystems berücksichtigt. Dementsprechend gibt Deloitte darüber kein Urteil ab.

| Kontroll-ID | Kontrollbeschreibung                                                                                                                                                                                                   | Resultat                                                                                                                                                                                                                                                                                                                                                                   | Managementstellungnahme                                                                                                                                                                                                                                                                                                                     |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.2         | <b>Zugriffsentzug</b><br><br>Ausgetretenen SBB-Mitarbeitenden wird der Zugriff auf SAP zeitnah entzogen.<br><br>Die Gültigkeit der SAP-Benutzer der externen Mitarbeitenden ist auf maximal 500 Tage beschränkt.       | Wir haben festgestellt, dass 15 externe Mitarbeitende im SAP-System von NOVA Abrechnung entgegen den Reglementen der SBB mehr als 500 Tage gültig waren.<br><br>Die 15 externen Mitarbeitenden sind alle in der kurz zuvor durchgeführten Überprüfung der Benutzerzugriffsrechte bestätigt wurden.                                                                         | <b>Implementierte, mitigierende Massnahme:</b><br><br>In der Zwischenzeit wurde die Gültigkeiten aller externen Benutzer auf die maximal zulässige Frist angepasst.<br><br><b>Zukünftige Massnahme:</b><br><br>Ein angepasster Prozess stellt zukünftig die zeitnahe Anpassung der Gültigkeitsdauer auf die maximal zulässige Dauer sicher. |
| 2.3         | <b>Überprüfung der Benutzerzugriffsrechte</b><br><br>Die kritischen Zugriffsberechtigungen werden regelmässig überprüft.                                                                                               | Wir haben eine Stichprobe von Berechtigungen geprüft, die während der Rezertifizierung von Rolleninhabern als unangemessen identifiziert wurden. Dabei haben wir festgestellt, dass in 5 von 25 Fällen die unangemessenen Berechtigungen erst nach ungefähr 30 Tagen entzogen wurden, wodurch der Berechtigungsentzug nicht zeitnah erfolgte.                              | <b>Implementierte, mitigierende Massnahme:</b><br><br>In der Zwischenzeit wurden alle Benutzeranpassungen umgesetzt.<br><br><b>Zukünftige Massnahme:</b><br><br>Bei der nächsten Durchführung der Überprüfung der Benutzerzugriffsrechte wird der zeitnahe Entzug sichergestellt.                                                           |
| 2.7         | <b>SAP_ALL und SAP_NEW</b><br><br>Dialog und Service Benutzern sind keine SAP_ALL oder SAP_NEW Profile dauerhaft zugeordnet.<br><br>Temporärer SAP_ALL/ SAP_NEW Zugang wird angefragt, genehmigt und zeitnah entzogen. | Wir haben festgestellt, dass ein Benutzer das hochprivilegierte Profil SAP_ALL zugewiesen war, welches die Ausführung aller Transaktionen in NOVA Abrechnung ermöglicht und gemäss SBB-Richtlinien nur kurzfristig und bei aktuellem Bedarf vergeben werden darf.<br><br>Im Rahmen unserer Prüfung haben wir jedoch festgestellt, dass der Benutzer nicht verwendet wurde. | <b>Implementierte, mitigierende Massnahme:</b><br><br>Das Profil SAP_ALL wurde in der Zwischenzeit entzogen und der Benutzer auf allen Systemen gesperrt.                                                                                                                                                                                   |

| Kontroll-ID | Kontrollbeschreibung                                                                                                                                             | Resultat                                                                                                                                           | Managementstellungnahme                                                                                                                         |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.8         | <p><b>Notfallberechtigungen</b></p> <p>Die Benutzung von Notfallberechtigungen werden protokolliert und bis spätestens am 15. Tag des Folgemonats überprüft.</p> | <p>Bei der Prüfung der Reviews von Notfallberechtigungs-Protokollen haben wir festgestellt, dass 19 Protokolle nicht zeitnah überprüft wurden.</p> | <p><b>Implementierte, mitigierende Massnahme:</b></p> <p>In der Zwischenzeit wurden alle Protokolle als angemessen beurteilt und bestätigt.</p> |



Dieses Dokument ist vertraulich und nur zu Ihrer Information hergestellt. Deshalb dürfen Sie ohne unsere schriftliche Einwilligung dieses Dokument niemandem weitergeben. Deloitte AG lehnt jegliche Haftung gegenüber Dritten ab, welche sich aus dem Zugang dieser Dokumente ergibt.

Deloitte AG ist eine Tochtergesellschaft von Deloitte NSE LLP, einem Mitgliedsunternehmen der Deloitte Touche Tohmatsu Limited («DTTL»), eine «UK private company limited by guarantee» (eine Gesellschaft mit beschränkter Haftung nach britischem Recht). DTTL und ihre Mitgliedsunternehmen sind rechtlich selbständige und unabhängige Unternehmen. DTTL und Deloitte NSE LLP erbringen selbst keine Dienstleistungen gegenüber Kunden. Eine detaillierte Beschreibung der rechtlichen Struktur finden Sie unter [www.deloitte.com/ch/about](http://www.deloitte.com/ch/about)

© 2024 Deloitte AG. All rights reserved