

Integrierte Assurance in der Praxis: Übersicht und Herausforderungen

Angie Hunziker, SBB Konzern-Risikomanagement
4.5.2022



Agenda & Ziele: Integrierte Assurance in der Praxis

Kurze Vorstellung Angie Hunziker	3'
Teil 1, Theorie: Definitionen und heutige Ansätze 🎯 Gemeinsames Verständnis schaffen	10'
Teil 2, Praxis: Integrierte Assurance bei SBB 🎯 Aufzeigen von Stand und Herausforderungen in der Praxis	10'
Q & A	7'

Begrüssung und Einleitung



Angie Hunziker
Leiterin SBB Konzern-
Risikomanagement

Beruflicher Werdegang

- SBB: Leitung Corporate Risk Management SBB
- SBB Infrastruktur: Divisional Risk Management
- Swiss International Air Lines: Central Controlling, Risk Management und IKS
- KPMG: Internal Audit, Risk & Compliance Services
- ABB: SOX-Koordination und -Verantwortung



Aus- und Weiterbildungen

- Weiterbildung zur zertifizierten Risikomanagement-Assessorin (CRMA)
- Weiterbildung zur zertifizierten Internen Revisorin (CIA)
- FHNW-Studium International Management / Business Administration, Schwerpunkt Accounting / Controlling



Teil 1: Theorie

Zugrundeliegende Definitionen

➡ Unter **Assurance** wird die Gesamtheit der in einem Unternehmen bestehenden Überwachungs- und Kontrollfunktionen verstanden. (KMPG 2012)

Ziel der Assurance-Funktionen ist es, der Unternehmensführung (Verwaltungsrat und Geschäftsleitung) eine **Sicherheit** bezüglich der Überwachung von Unternehmensrisiken und der Einhaltung von gesetzlichen und internen Vorgaben zu bieten. (SBB)

GRC ist ein integrierter, holistischer Ansatz für organisationsweite Governance, Risk und Compliance, der gewährleistet, dass die Organisation sich **ethisch** und gemäss ihrem **Risikoappetit** sowie **interner und externer Vorgaben** verhält (...), wodurch Effizienz und Effektivität gesteigert werden. (Racz et al. 2010)

➡ **Corporate Governance** bezeichnet Grundsätze und Regeln, mit deren Hilfe die Strukturen und das Verhalten der obersten Führungskräfte gesteuert und überwacht werden können. (SECO 2021)

➡ **Risikomanagement** bezweckt den systematischen, aktiven, zukunfts- und zielorientierten Umgang mit wesentlichen Risiken eines Unternehmens. (SBB)

Compliance bedeutet die Einhaltung von gesetzlichen, regulatorischen und internen Vorschriften sowie die Beachtung von marktüblichen Standards (Regeltreue). (SBB)

Teil 1: Theorie

Definition zu integrierter (combined) Assurance

Combined Assurance entspricht einer koordinierten und integrierten Zusammenarbeit aller unternehmerischer Funktionen, die direkten oder indirekten **Risikobezug** haben und zur Verbesserung der **Governance-Struktur** beitragen können.

Zielsetzung ist es hierbei, entweder den **Ressourcenaufwand** der Governance-Funktionen zu minimieren oder die **Leistung** ceteris paribus zu maximieren.

Ergänzend kann die Zusammenarbeit mit Governance-relevanten externen Funktionen weitere risikorelevante Bereiche einbinden.

Durch die Erfüllung der Zielsetzung steigert Combined Assurance die **Qualität der Corporate Governance**.

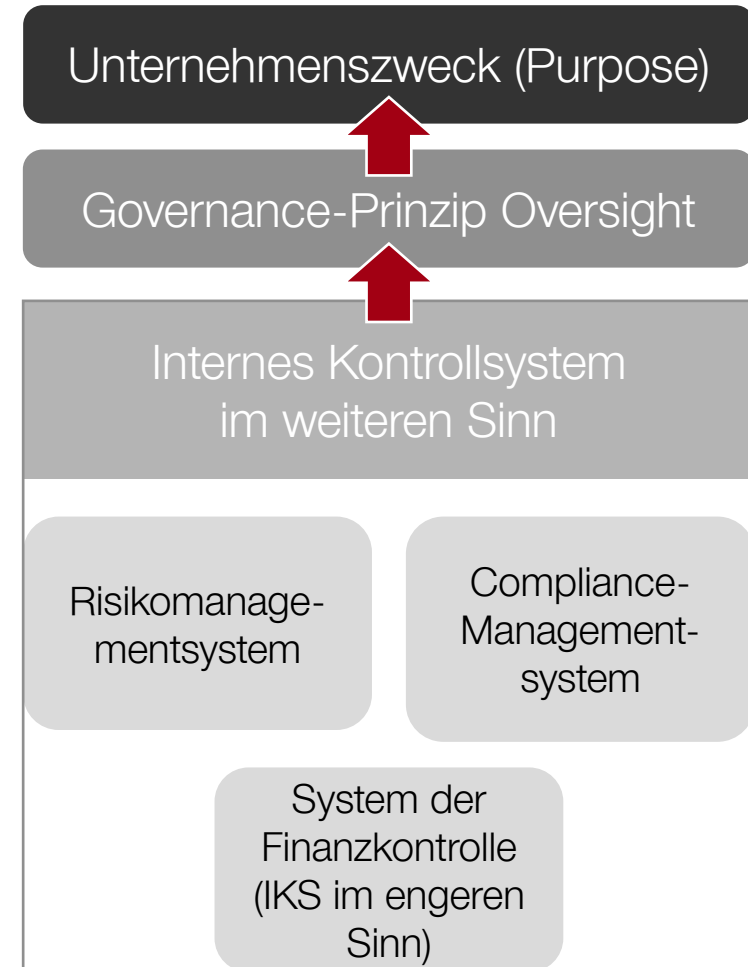
(Eulerich 2016 sowie DIIR 2020)

Teil 1: Theorie

Ansätze im Zusammenhang mit integrierter Assurance (1/2)

ISO 37000 (2021) Governance of organizations

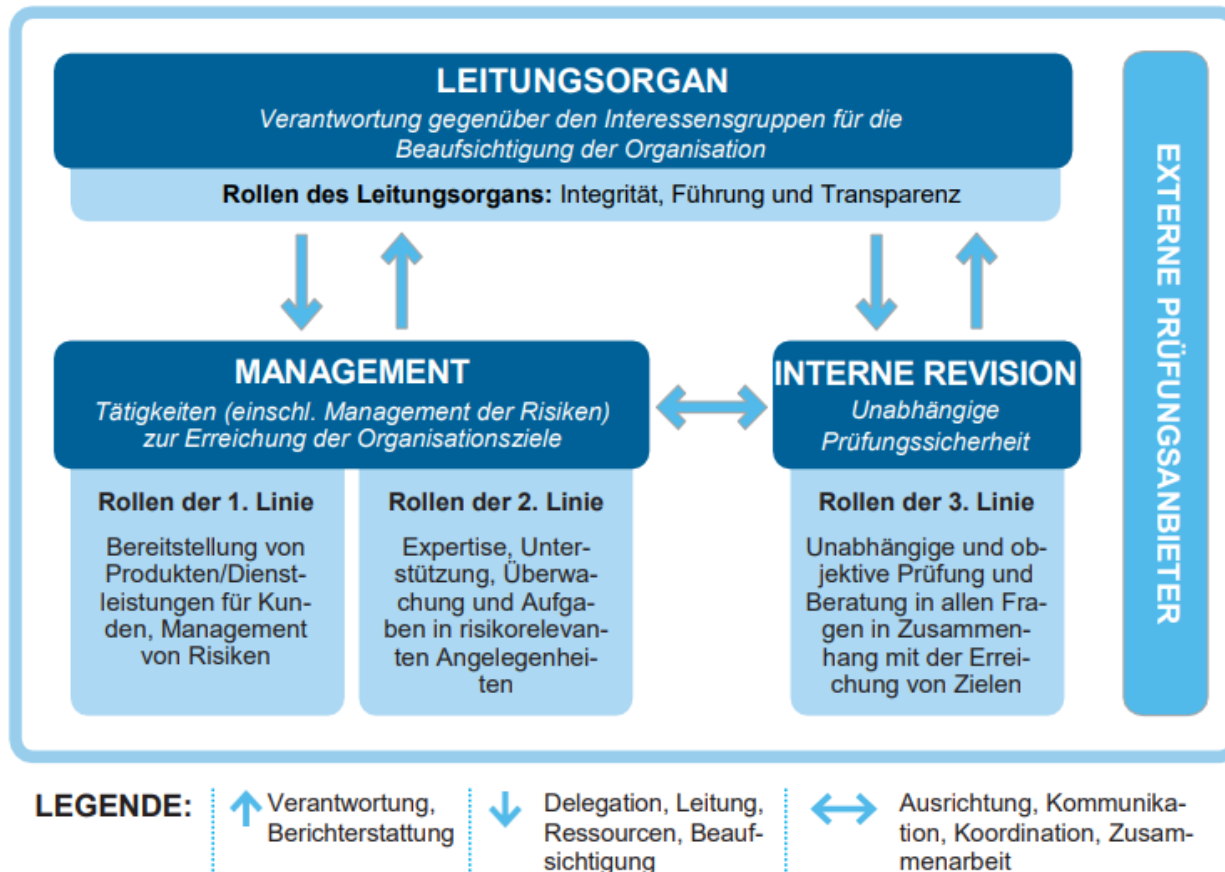
- Erster globaler Standard zur guten Governance
- Der Standard unterstützt das oberste Organ (governing body) dabei, eine **integrale Governance** einzuführen, um wirksam, sozial verantwortlich und ethisch den Unternehmenszweck (purpose) zu erreichen.
- Gute Corporate Governance bildet so die Grundlage für langfristigen Unternehmenserfolg.
- Ein zentrales Element des Governance-Prinzips **Oversight** ist ein internes Kontrollsystem bestehend aus **Risikomanagementsystem, Compliance-Managementsystem und System der Finanzkontrolle** (IKS im engeren Sinn).



Teil 1: Theorie

Ansätze im Zusammenhang mit integrierter Assurance (2/2)

Das Drei-Linien-Modell des IIA (2020)



- Assurance wird erstmals explizit definiert als «**unabhängige Bestätigung und Vertrauen**».
- Vertrauen ist selten absolut; Assurance kann nur angemessen sein («reasonable»).
- Die Rollen der dritten Linie umfassen somit Assurance und Beratung in Bezug auf die Angemessenheit und Wirksamkeit der Governance und des Risikomanagements.
- **Assurance wird explizit der dritten Linie zugeordnet.**

(Ruud et al. 2020)

Teil 1: Theorie

Würdigung und Weiterentwicklung der heutigen Ansätze

- Das Drei-Linien-Modell erschwert durch seine strikte Trennung von Governance-Funktionen eine integrierten Assurance.
- ISO 37000 stellt das Interne Kontrollsystem ins Zentrum und vernachlässigt zusätzliche Assurance-Funktionen, die für eine erfolgreiche Unternehmensführung wichtig sind.
- Es bietet sich an, eine **Übersicht** der erweiterten Assurance-Funktionen zu gewinnen.
- Die Zusammenarbeit gestaltet sich unterschiedlich; das Ziel – gemäss Definition:
 - **Synergien schaffen:** Ressourcenaufwand der Governance- / Assurance-Funktionen minimieren bzw. Leistung maximieren.
 - **Governance** stärken und ein **wirksames Risikomanagement** ermöglichen.
- Einsatz eines **Chief Assurance Officer / Assurance-Koordinationsstelle** für die Zielerreichung förderlich. (KMPG 2012)

Teil 1: Theorie

Voraussetzungen und Hindernisse

Vorteilhafte Rahmenbedingungen für eine erfolgreiche integrierte Assurance



- Organisatorische Zusammenführung bzw. vorteilhafte Organisationsstruktur
- Angemessene Aufstellung vis-à-vis Unternehmensgrösse
- Geeignete Unternehmens- / Zusammenarbeitskultur
- Einheitliches Risikoverständnis
- Durchgängige Methodik, zentrale Ablage (Tool)

Aktuelle Hindernisse



- Ungenügender Einbezug der externen Revision / Regulators
- Kreation von «Silos» infolge der rigiden Organisationsstrukturen
- Oft reaktive Verteidigungsaktivitäten anstelle von proaktivem Ansatz
- Ungenügende Bereitschaft und Qualität der Kooperation
- Abstimmungen mit grossem Aufwand verbunden

(ZHAW 2019 sowie eigene Würdigung A. Hunziker)

Die Praxis hat schon viele Theorien erlebt.

Hans-Jürgen Quadbeck-Seeger (2006), Chemiker, Mitglied des Deutschen Bundestages

Teil 2: Praxis

Konzernziele SBB



Kunden-
pünktlich-
keit



Sicherheit



Jahres-
ergebnis



Kunden-
zufrieden-
heit



Konzern-
image



Personal-
motivation



Free
Cashflow



Markt-
leistung



Ökologische
Nachhaltig-
keit

Teil 2: Praxis

Integrierte Assurance bei SBB: Fokus auf interne Anbieter

Folgende **interne Funktionen** bieten bei SBB mindestens teilweise Assurance:

- Interne Revision
- Risikomanagement
- Compliance
- Internes Kontrollsystem
- Sicherheit (Safety)
- Information Security
- Security
- Business Continuity Mgmt.

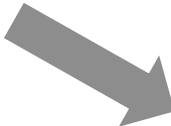
Als **Third Line-Assurance-Funktion** prüft die Interne Revision u.a. die Funktionsfähigkeit der Management-Systeme (Wirksamkeit der Second Line).

Second Line-Assurance-Funktionen betreiben (konzernweite) Management-Systeme inkl. Erlass und Operationalisierung von Vorgaben sowie Überwachung. Beratend unterstützen diese die First Line bei der Umsetzung.

Teil 2: Praxis

Organisation SBB

Verwaltungsrat SBB AG Monika Ribar	
CEO SBB AG Vincent Ducrot*	Interne Revision Stefan Raimann



	Markt Personenverkehr Véronique Stephan*	Produktion Personenverkehr Linus Looser*	Immobilien Alexander Muhm*	Infrastruktur Peter Kummer*	Segment Güterverkehr Nicolas Perrin**
Finanzen Franz Steiger*					SBB Cargo AG Désirée Baer
Human Resources Markus Jordi*					
Informatik Jochen Decker*					SBB Cargo International AG Sven Flore
Kommunikation Andreas Stuber					
Unternehmensentwicklung Urs Wälchli					
Sicherheit und Produktionsqualität Heidrun Buttler					
Recht und Compliance Stephanie Bregy					
Public Affairs & Regulation Bernhard Meier					

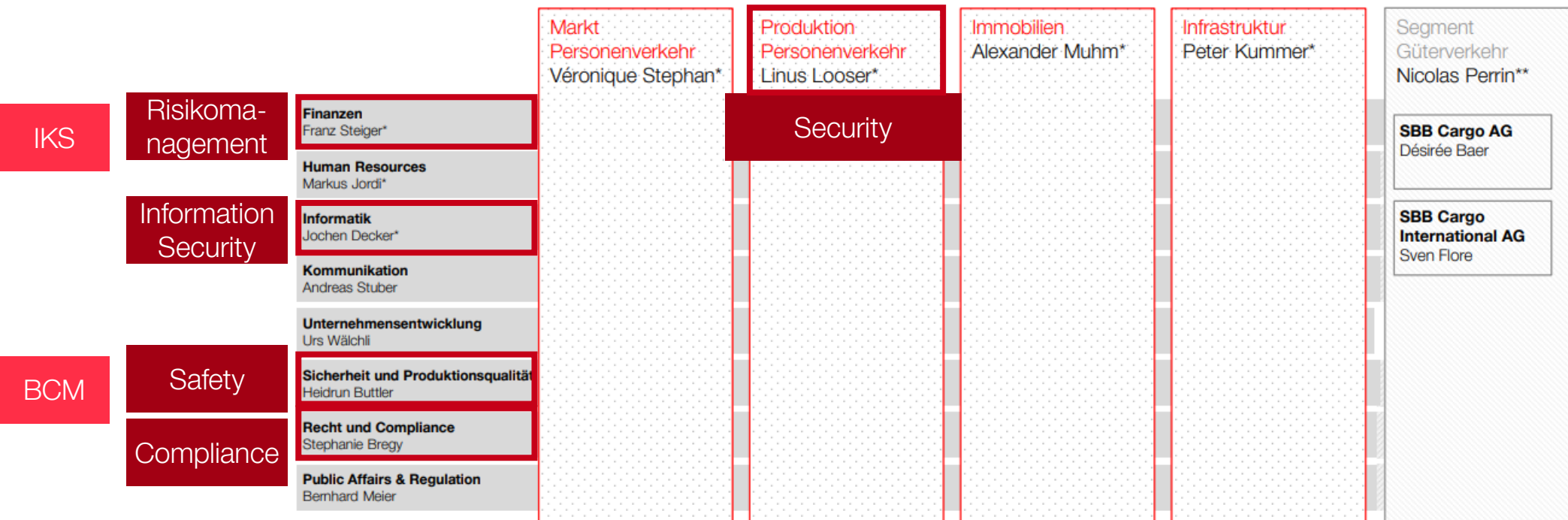
Division

Fachführung

* Mitglied der Konzernleitung ** Segmentsverantwortung

Teil 2: Praxis

Integrierte Assurance bei SBB: Organisatorische Einbettung



Division

Fachführung

* Mitglied der Konzernleitung ** Segmentsverantwortung

Teil 2: Praxis

Integrierte Assurance bei SBB: Zusammenarbeit

Wir fokussieren auf und evaluieren diese sechs **Zusammenarbeitsbereiche**:

Regelmässiger,
systematisierter
Informationsaus-
tausch

Abgestimmte
Prozesse

Durchgängige
Tool-Landschaft

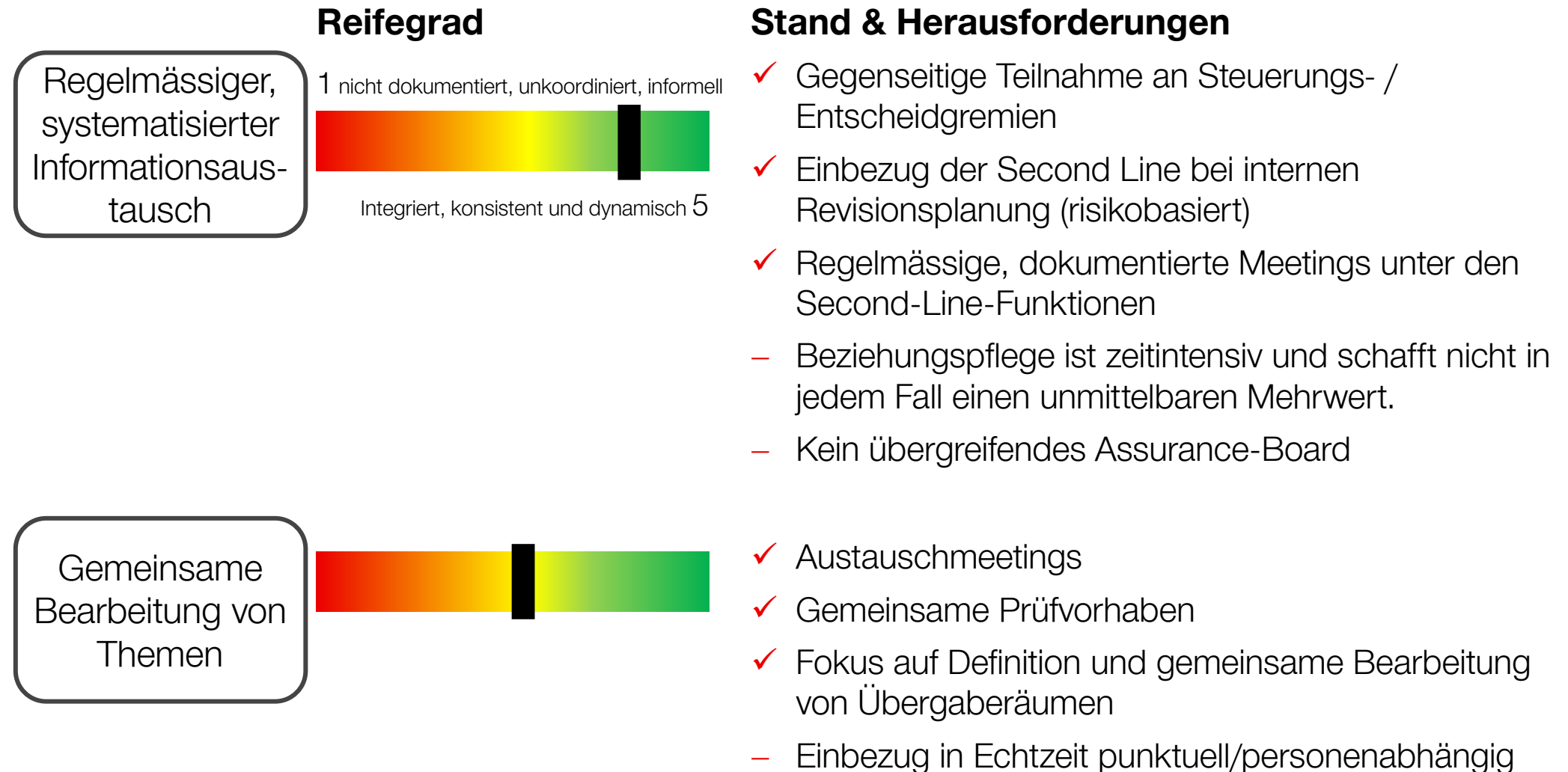
Gemeinsame
Bearbeitung von
Themen

Integrierte
Berichterstattung

Gesamtheitliches
Management-
system

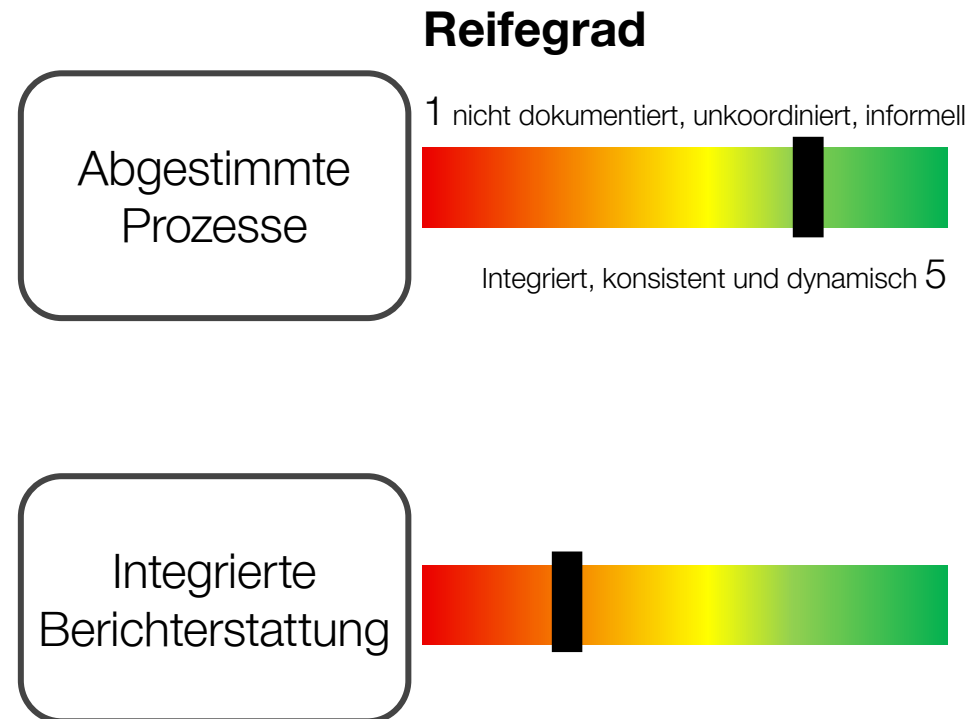
Teil 2: Praxis

Integrierte Assurance bei SBB: Würdigung (1/3)



Teil 2: Praxis

Integrierte Assurance bei SBB: Würdigung (2/3)



Stand & Herausforderungen

- ✓ Konzern-Risk-Prozesse bauen mehrheitlich auf den vorgelagerten First- und Second-Line-Risikobeurteilungen auf.
- ✓ Das Risikomanagement der SBB ist durchgängig.
- Aufeinander abgestimmte Prozesse lassen wenig Raum für Dynamisierung.
- ✓ Aufbau eines integrierten Konzernlagemonitorings mit aktuellen Bedrohungslagen, Zusammenspiel der Second Line
- ✓ Jahresberichte sind zeitlich synchron ...
- ... aber separat und inhaltlich nur minimal aufeinander abgestimmt.

Teil 2: Praxis

Integrierte Assurance bei SBB: Würdigung (3/3)

Reifegrad

Durchgängige
Tool-Landschaft



Gesamtheitliches
Management-
system



Stand & Herausforderungen

- ✓ Beschaffung eines GRC-Tools für folgende Management-Systeme:
 - ✓ Risk Management-System
 - ✓ Internes Kontrollsystem
 - ✓ Compliance-Managementsystem
 - ✓ Information Security Management System
 - ✓ Schnittstelle zum BCM-System
- Unsicherheiten zum Rollout [in First Line]
- ✓ Harmonisierte Risk-Methodik, abgestimmte Prozesse, durchgängiges Tool
- ✓ Zweimal jährlich gesamtheitliche Risikosicht
- Wenig Weisungen zu Assurance
- Ausblick: Erweitertes IKS mit Kontrollen aller Assurance-Funktionen

Q & A

Kontakt:

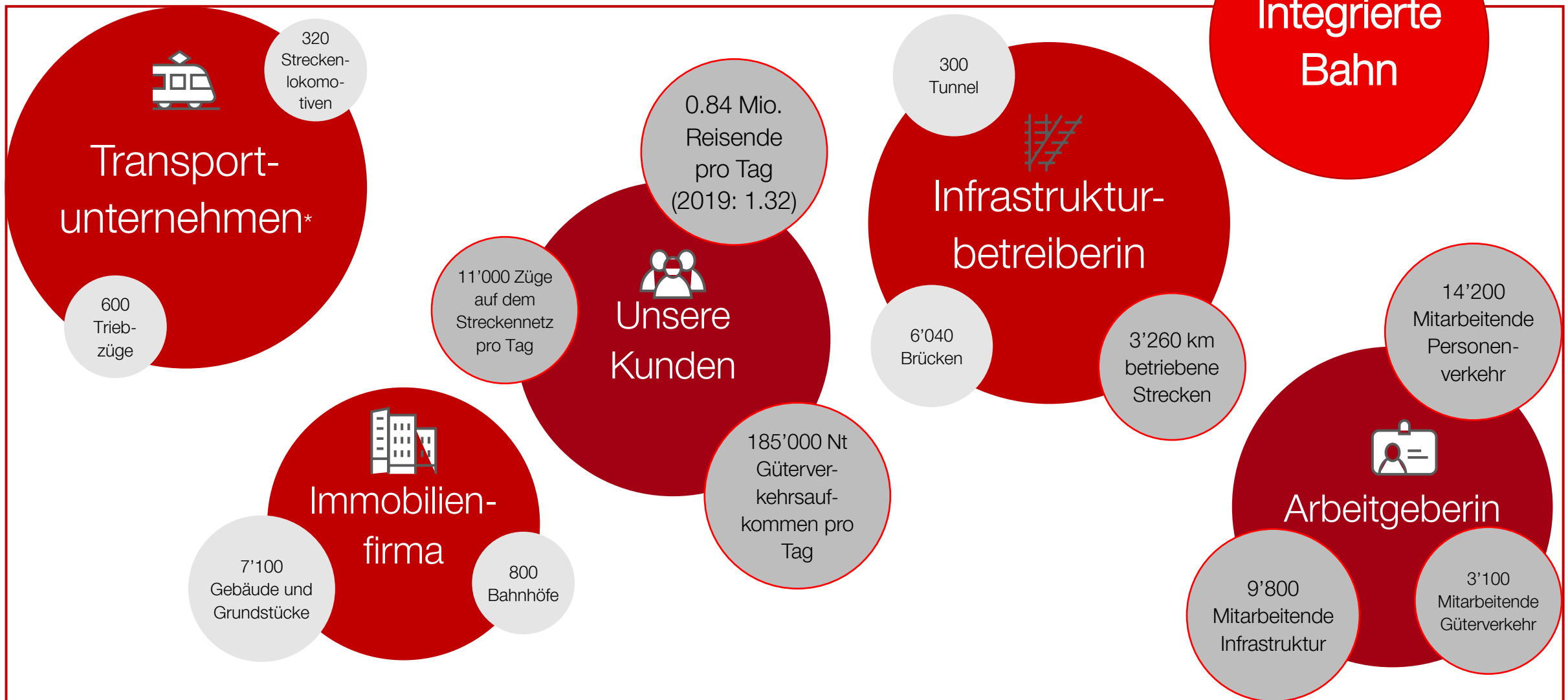
angela.hunziker@sbb.ch

+41 79 776 17 71



Danke, merci, grazie!

Die SBB in Zahlen und Fakten



Zahlen sind gerundet, Stand 2019 (exkl. COVID-19-Effekte)

* Transportunternehmen inkludiert die Beförderung von Passagieren als Eisenbahnverkehrsunternehmen (SBB Personenverkehr) wie auch den Transport von Gütern (SBB Cargo)

Quelle: Zahlen und Fakten ([sbb.ch](https://www.sbb.ch))