

A long-exposure photograph of a city street at night, showing light trails from traffic and streetlights. The scene is dominated by warm yellow and orange tones from the lights, with some cooler blue tones from the sky and building windows. The street is wide and has multiple lanes with white directional arrows. Tall buildings line both sides of the street, some with lit windows. Traffic lights are visible in the distance, and a few street signs are on the right side. The overall atmosphere is busy and urban.

# RISIKOBASIERTE COMPLIANCE BEI DER POST

WIEVIEL RISIKO VERTRÄGT COMPLIANCE?

Markus Schumacher, Leiter GRCS (Governance, Risikomanagement, Compliance, Sicherheit)  
Die Schweizerische Post AG  
13. September 2023



# Agenda

1

## Einstieg

Risikobasierte Compliance

2

## CMS Post

Compliance bei der Schweizerischen Post

3

## Schluss

Take Aways und Action Points



# Risiko und Compliance Übersicht



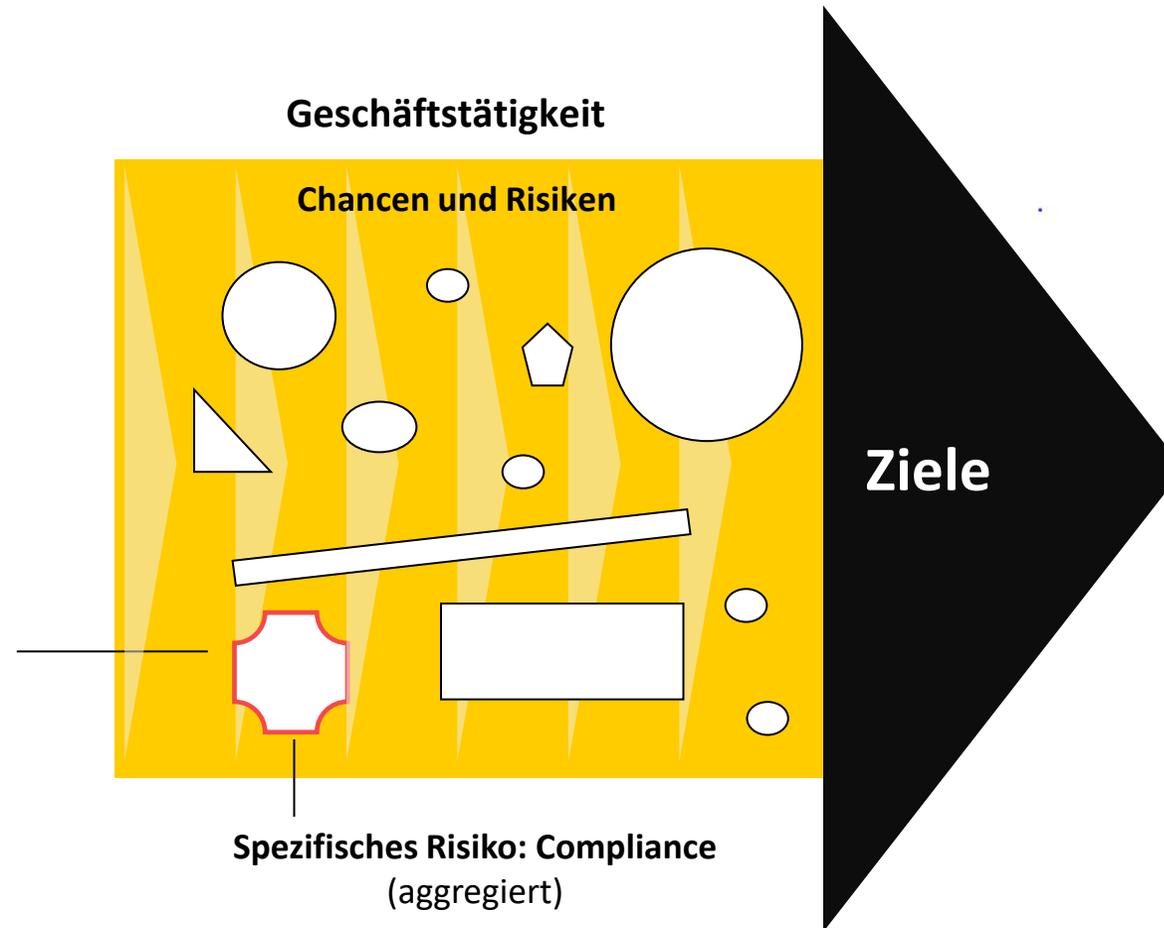
## Ressourcen:

- Human Ressourcen
- Kapital
- Betriebsmittel, etc.



## Rahmenbedingungen:

- Absatz-, Beschaffungs-  
Kapital-, Arbeitsmärkte
- **Gesetze und Vorgaben**
- Umwelt, Politik, etc.



**Die korrekte Einhaltung von Gesetzen und Vorgaben (Compliance) ist eines von vielen Risiken der Geschäftstätigkeit (meist eines der Grösseren)**



# Risiko und Compliance

## Verantwortung für Compliance-Risiken



**Gesamtverantwortung**  
VR und GL



Report



**Systemverantwortung**  
Compliance-Funktion

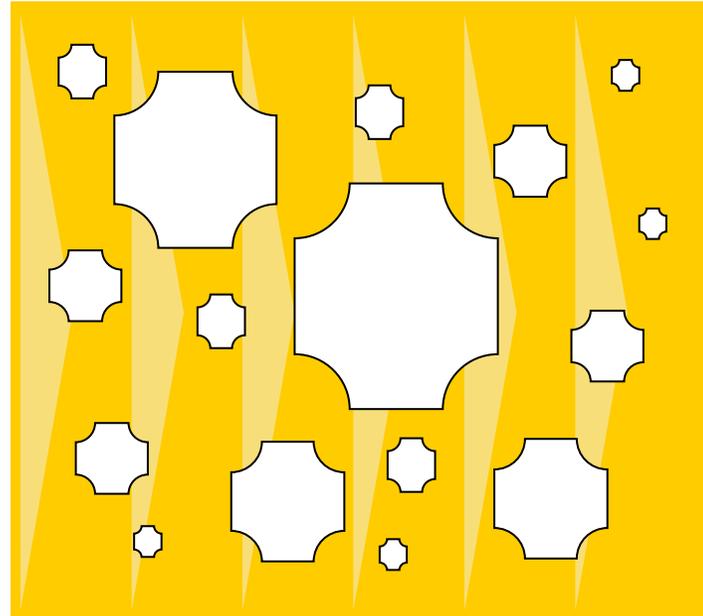


Support



**Einzelverantwortung**  
Vorgesetzte/Mitarbeitende

**Verschiedene  
Compliance-Risiken**



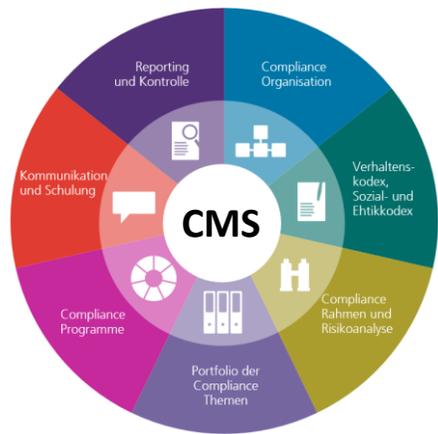
**Ziele**



**Ziele sind auf integre Art und Weise und unter Einhaltung von Gesetzen/Vorgaben zu erreichen.  
Die Verantwortung für Compliance-Risiken liegt bei den Organen bzw. den handelnden Personen**

# Risiko und Compliance

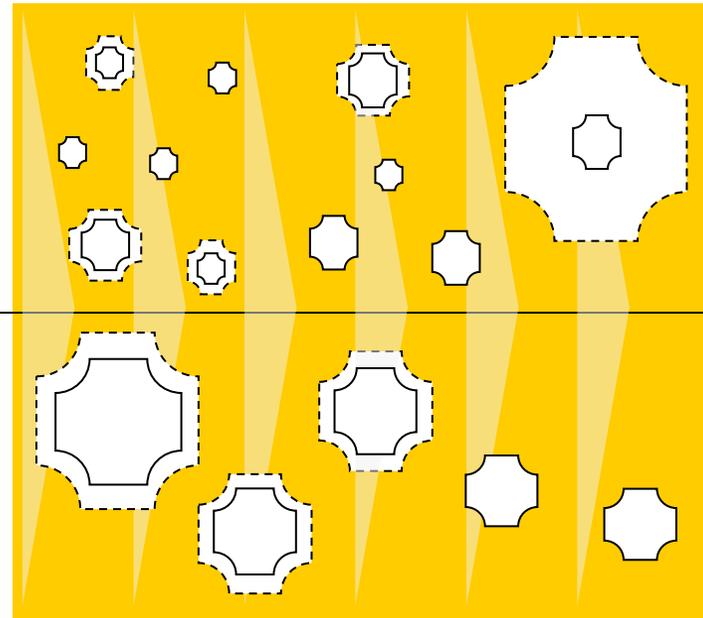
## Compliance-Management-System (CMS)



kleinere  
Compliance  
Risiken

grössere  
Compliance  
Risiken (CMS)

Compliance-Risiken  
risikobasiert gruppiert



Ziele



Netto-Risiko (nach Massnahmen)

Brutto-Risiko (vor Massnahmen)

**Das CMS identifiziert risikobasiert die grossen Compliance-Risiken und stellt ein System zur Verfügung, um diese Risiken zu bewirtschaften (Massnahmen, Kontrollen, Berichterstattung, etc.)**



# Risiko und Compliance

## Wieviel Risiko verträgt Compliance?

### Compliance & Risiko

- Compliance wurde «erfunden», um mit spezifischen (insb. legalen) geschäftsinhärenten Risiken **strukturiert** umzugehen
- Compliance **identifiziert** Risiken im Rahmen einer Risikoanalyse und agiert **risikobasiert**, d.h. die Aktivitäten werden auf die grossen Risiken (Existenz, Reputation) fokussiert
- Compliance **reduziert** Risiken (jedoch nicht auf Null – Entscheidungsfähigkeit und Effizienz sind zu wahren). Compliance kann einen Vorfall nicht ausschliessen
- **Analogie:** Bauen und Fliegen ist risikobehaftet aber unverzichtbar. Die Risiken werden so weit wie möglich reduziert

**Compliance verträgt sehr viele Risiken bzw. ist ein Verfahren, um mit Risiken umzugehen**

### CMS & Risiko

- Das CMS ist so zu betreiben, dass es seinen **Zweck** erfüllen kann (Nachweis Sorgfalt)
- Das CMS kann im **Reifegrad** variieren. Ein der Komplexität/Grösse des Unternehmens angemessener Reifegrad muss aber erreicht werden
- Risiken im CMS fallen auf das Unternehmen, die Organe und die Compliance-Funktion zurück
- **Analogie:** Im Bau und in der Fliegerei wurden Systeme/Prozeduren entwickelt, um mit den Risiken umzugehen. Mit deren Anwendung werden Risiken reduziert und die verlangte Sorgfalt nachgewiesen

**Das CMS muss sorgfältig betrieben werden und verträgt nur beschränkte Risiken**



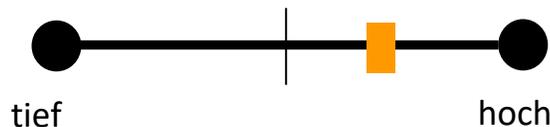
# Risiko und Compliance

## Risk-Taking in der Compliance

### Risk-Taking 1. Ebene



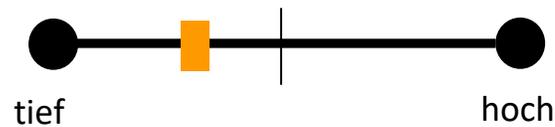
Umfang der «Investition» in eine allgemeine Kultur der Regeltreue und der Integrität



### Risk-Taking 2. Ebene



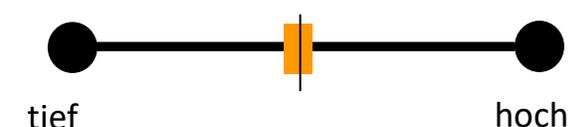
Umfang der aufgrund einer Risikoanalyse identifizierten «grossen» Compliance-Risiken, die im Rahmen eines CMS bewirtschaftet werden



### Risk-Taking 3. Ebene



Umfang der innerhalb eines einzelnen Compliance-Themas (Programm) durchgeführten Massnahmen zur Verminderung des spezifischen Compliance-Risikos



# Agenda

1

## Einstieg

Risikobasierte Compliance

2

## CMS Post

Compliance bei der Schweizerischen Post

3

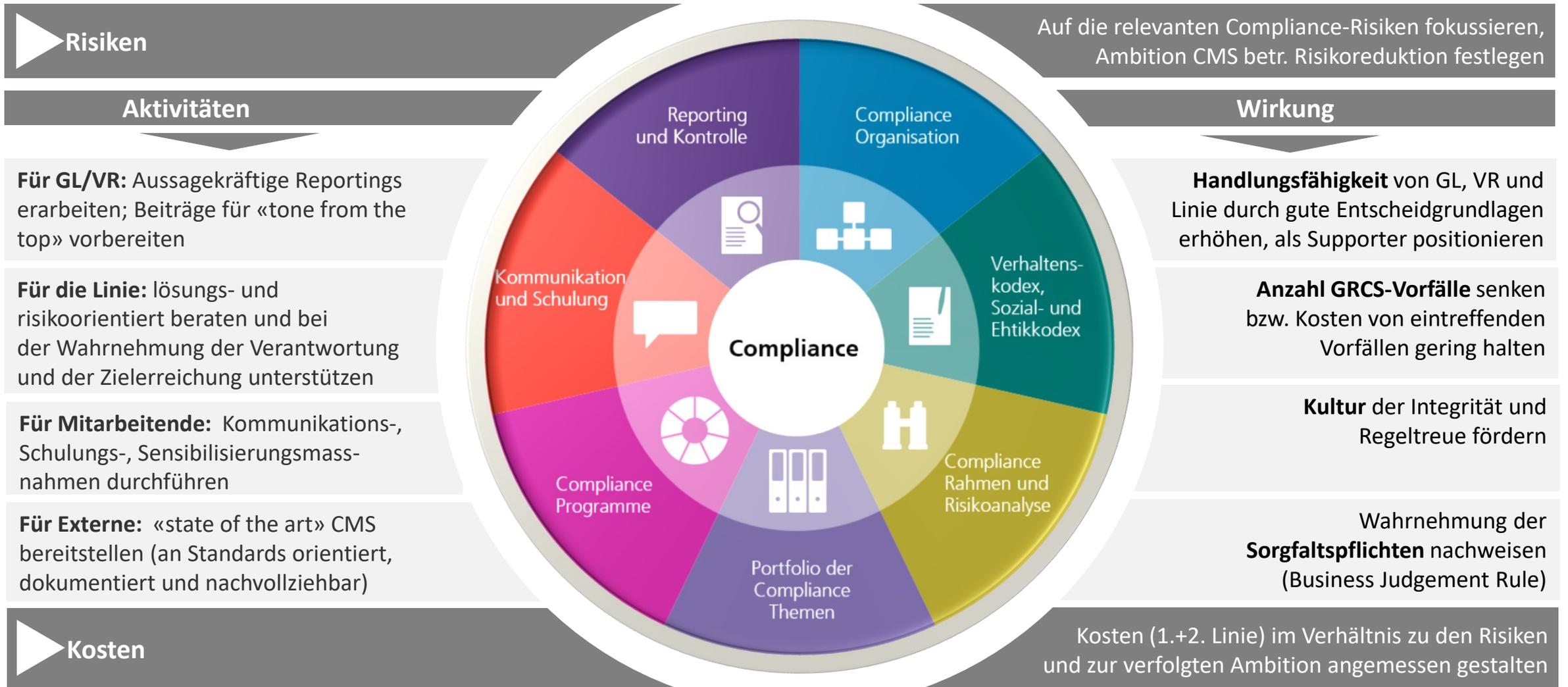
## Schluss

Take Aways und Action Points



# Compliance Management System Post

Ziel: Angestrebte Risikoreduktion mit verhältnismässigen Kosten erreichen



# Risiko und Compliance

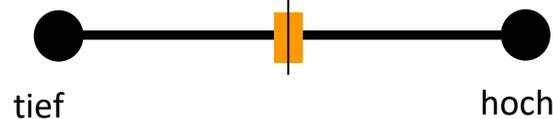
## Risk-Taking in der Compliance Post

### Risk-Taking 1. Ebene

«Investition» in eine allgemeine Kultur der Regeltreue und der Integrität



- Verhaltenskodex
- Kommunikationsmassnahmen
- Umgang mit Verstössen
- Vorgaben

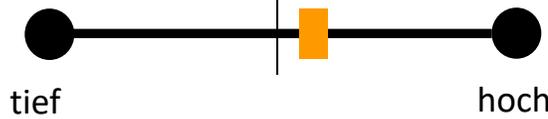


### Risk-Taking 2. Ebene

Compliance-Risiken, die im Rahmen eines CMS bewirtschaftet werden (Programme)



- Beschaffungsrecht
- Wettbewerbsrecht
- Subventionsrecht
- Datenschutz
- Antikorruption
- Postrecht

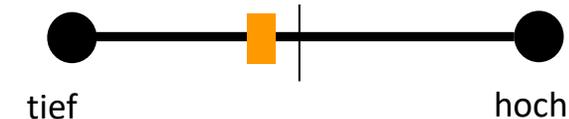


### Risk-Taking 3. Ebene

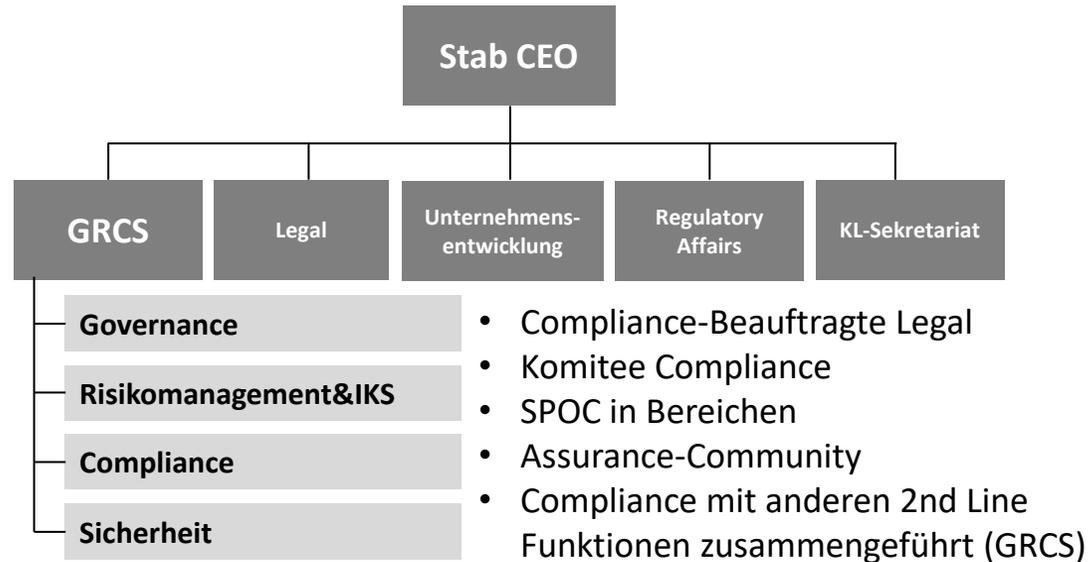
«Massnahmendichte» innerhalb eines Compliance-Programms



- Fokus auf Ziele und Vorgaben sowie auf Aufgaben, Kompetenzen und Verantwortungen
- Kontrollen im Aufbau



# Compliance als Teil der Assurance Organisation



## Kriterien Assurance-Funktion

**VR/GL  
verpflichtet**

- Fokus auf Organe mit Gesamtverantwortung
- Direkter Zugang zu Organen (VR, GL)

**systematisch**

- Eigenständige Risikoanalyse
- Systematischer Ansatz/Vorgehensmodell

**unabhängig**

- Formeller Auftrag
- Auskunfts-, Zugangs-, Einsichtsrecht
- Von Geschäftsaktivitäten organisatorisch getrennt
- Genügend Ressourcen

# Compliance Post

## Einordnung

### Was läuft gut ...

- Risikobasierte Herangehensweise
- Risikomitigation im Verhältnis zu Kosten
- Klare Rollen (1st und 2nd Line) und Dialog zu Ambition
- Zusammenarbeit mit anderen 2nd Line Funktionen und mit der Assurance Community
- Prinzipienorientiertes Vorgabewesen



### Woran arbeiten wir ...

- Reaktionszeit auf Veränderungen von Risiken
- Gemeinsames Verständnis zur Ambition des CMS und dafür notwendigen Investitionen und Massnahmen
- Abgestimmte Kommunikation über alle Ebenen
- Compliance-Kultur: Förderung Bewusstsein, Umgang mit Verstößen



# Agenda

1

## **Einstieg**

Risikobasierte Compliance

2

## **CMS Post**

Compliance bei der Schweizerischen Post

3

## **Schluss**

Take Aways und Action Points



# Zusammenfassung

## Was sind die Take Aways und die Action Points?

### Take Aways

1

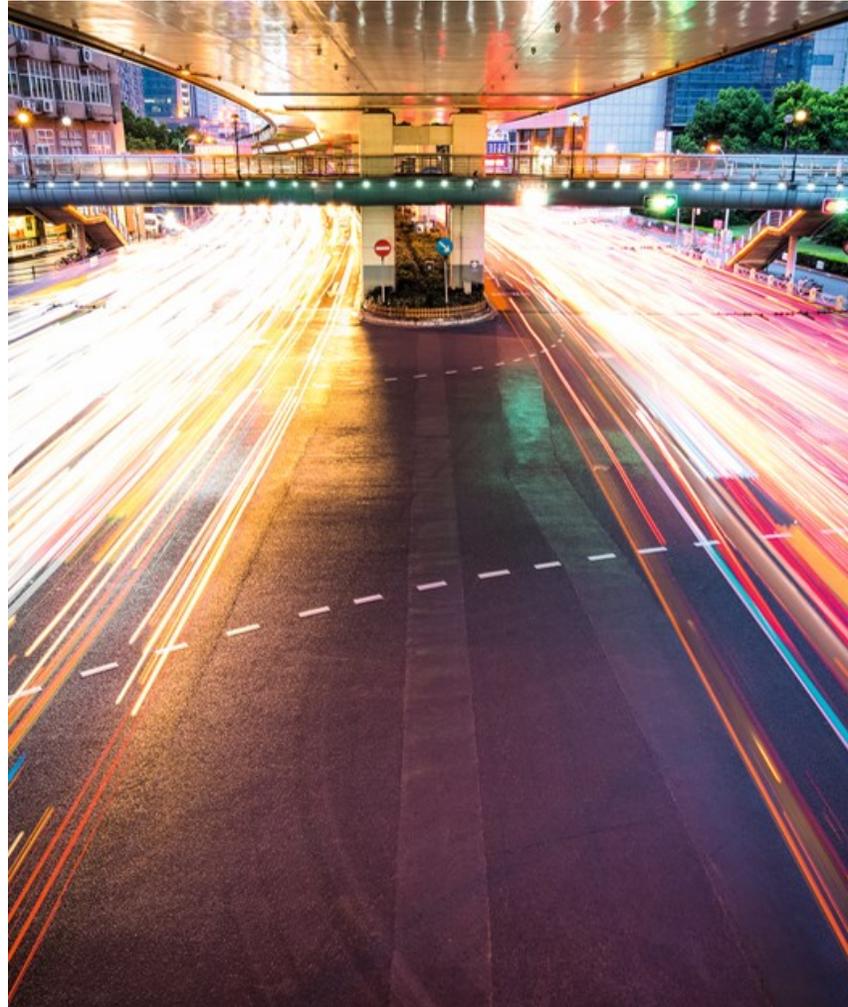
Compliance ist **risikobasiert** und damit unternehmerisch. Es geht um die grossen Risiken (Existenz, Reputation)

2

Im **CMS** werden die grossen **Risiken bearbeitet**. Das CMS muss sich an Grösse und Komplexität des Unternehmens orientieren. Es geht um den **Nachweis** der Wahrnehmung der **Sorgfaltspflichten**

3

Die **Balance** zwischen unternehmerischem Risiko und administrativem Overkill ist dann gefunden, wenn die **relevanten** Risiken im CMS mit **genügender** Sorgfalt bearbeitet werden



### Action Points

Regelmässige **Definition** der grossen Risiken im Rahmen einer Risikoanalyse

Regelmässige **Überprüfung** des CMS im Rahmen von internen und externen Revisionen

Das **CMS** nur **so gross wie nötig** machen («weniger ist mehr»). Die übrigen Risiken der 1st Line überlassen. Dafür in eine **Kultur** der Integrität investieren