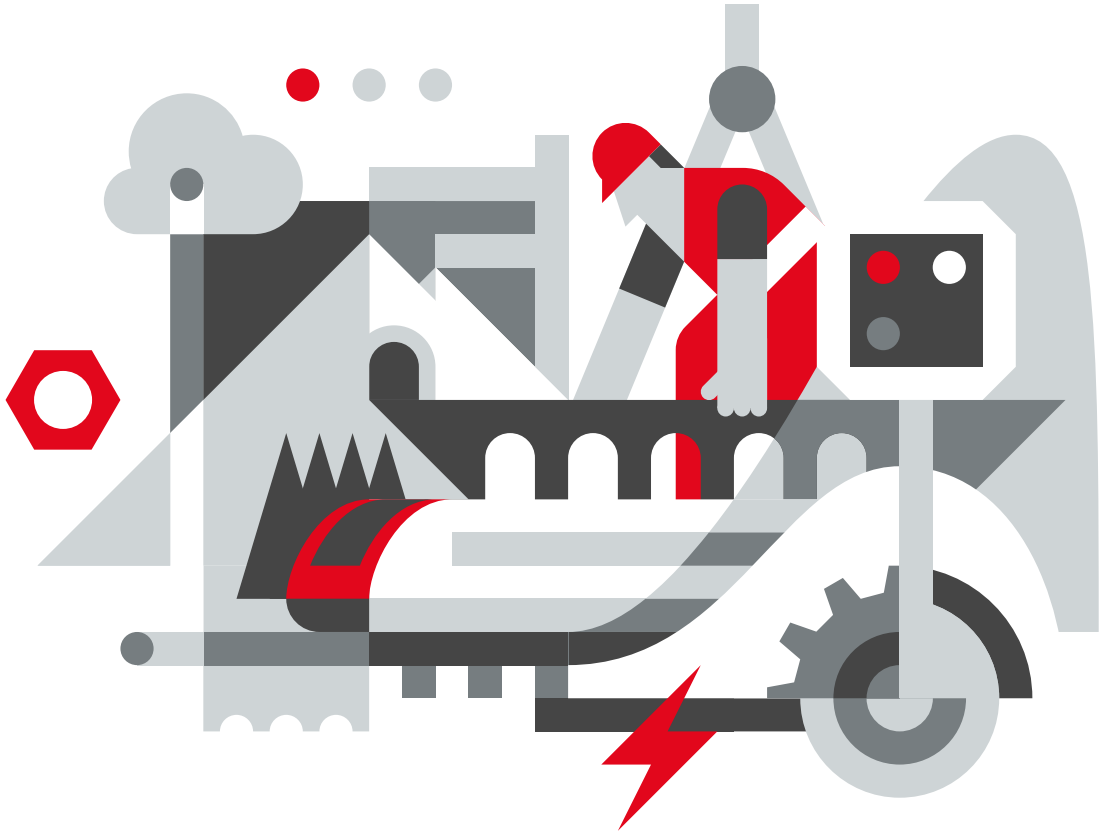
SWISSRAIL
Industry Association

Together for the Swiss Rail and Mobility Industry.

National. Global.



RAILplus Cyber Day
10. Juni 2024

Trend #1: Die 4. Industrielle Revolution

Erste mechanische Webmaschine | 1784

Ende des 18. Jhd. (Mechanisierung)

Erstes Fliessband, Schlachthäuser | 1870

Beginn des 20. Jhd. (Elektrifizierung)

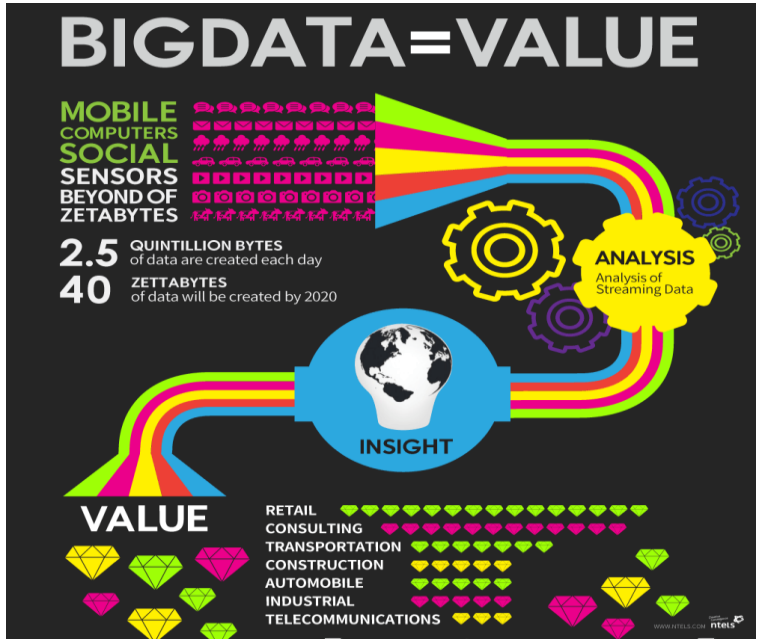
Erste speicherprogrammierbare Steuerung | 1969

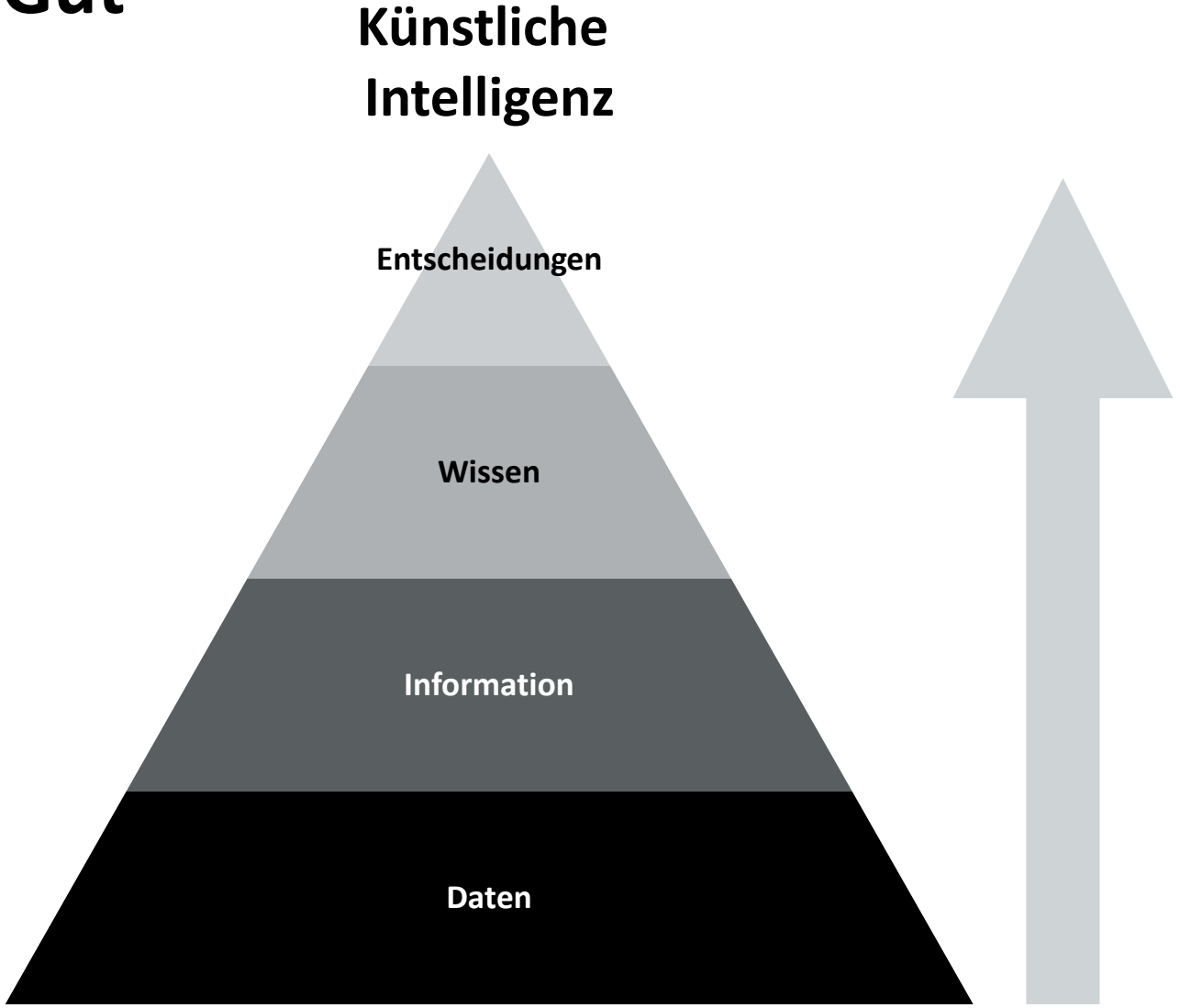
Beginn der 70er (Automatisierung)

Industrie 4.0

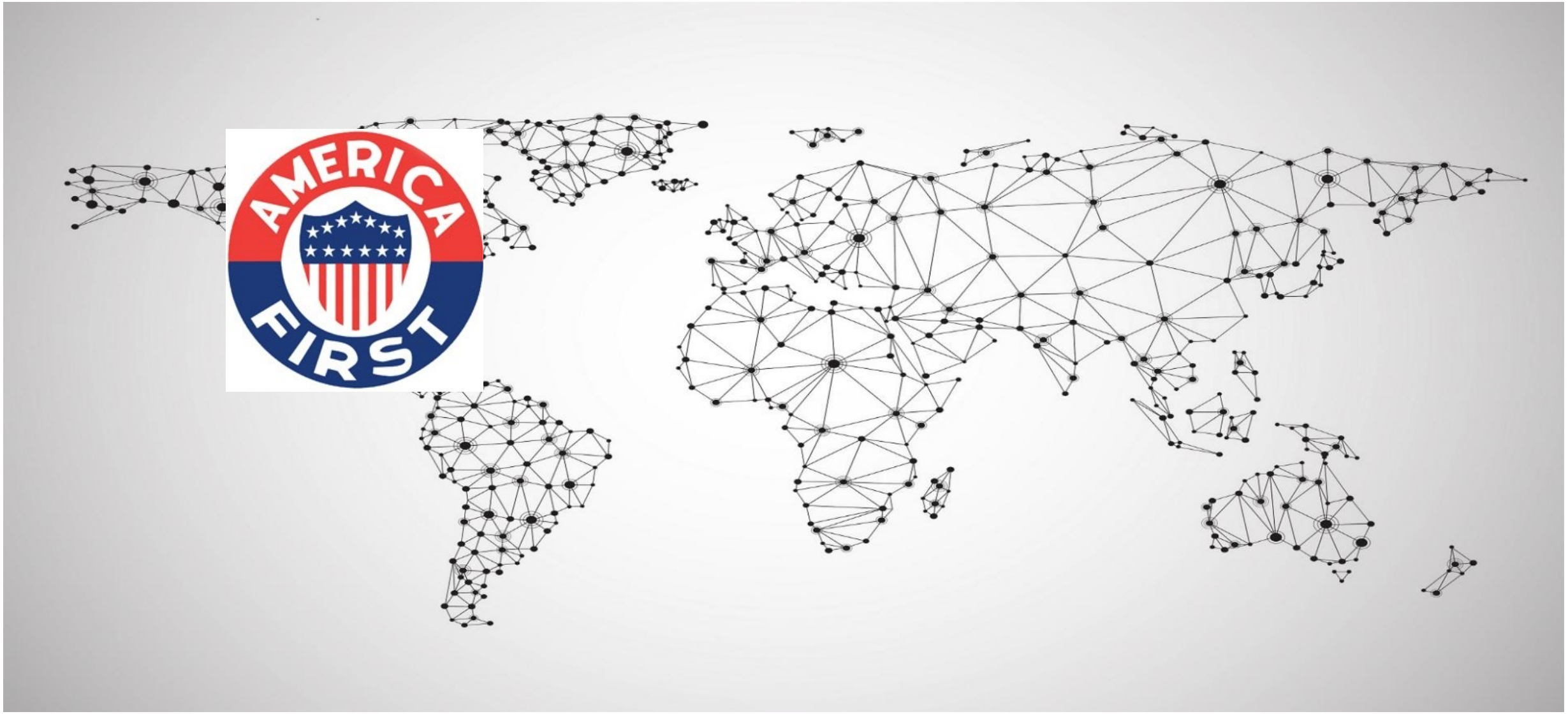
Heute (Vernetzung)

Trend #2: Daten als primäres Gut





Trend #3: Netzwerke, Anforderungen an lokale Inhalte



Trend #4: Disruptive Technologie

Innovations- und Produktionszyklen werden verkürzt

→Verkürzte Entwicklungszeit
→Agile Methoden

Trend #5: Grüne Bewegung

Trend #6: Wandel des Humankapitals

Trend #7: Wandel der Sozialen Werte

Diszipliniert konservativ

Unabhängige Anpassung an Wandel

Unabhängige Anpassung an Wandel

Mit Technologie aufgewachsen

Technologie angeboren

Trend #8: Automatisierung

Trend #9: Integrierter Mobilitätsansatz & Smart City

Resultat: Hohe Sicherheitskomplexität

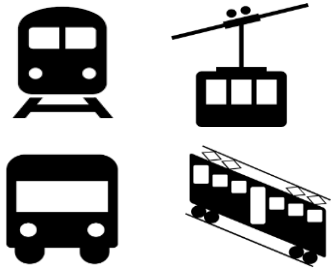
Safety

Security

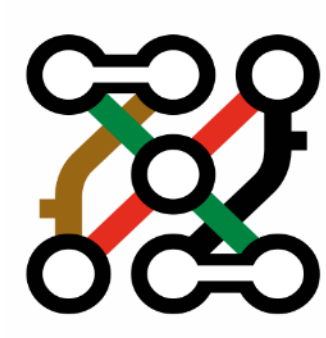
Zusammenbringen von Stakeholders

Industrie

Betreiber



Behörden



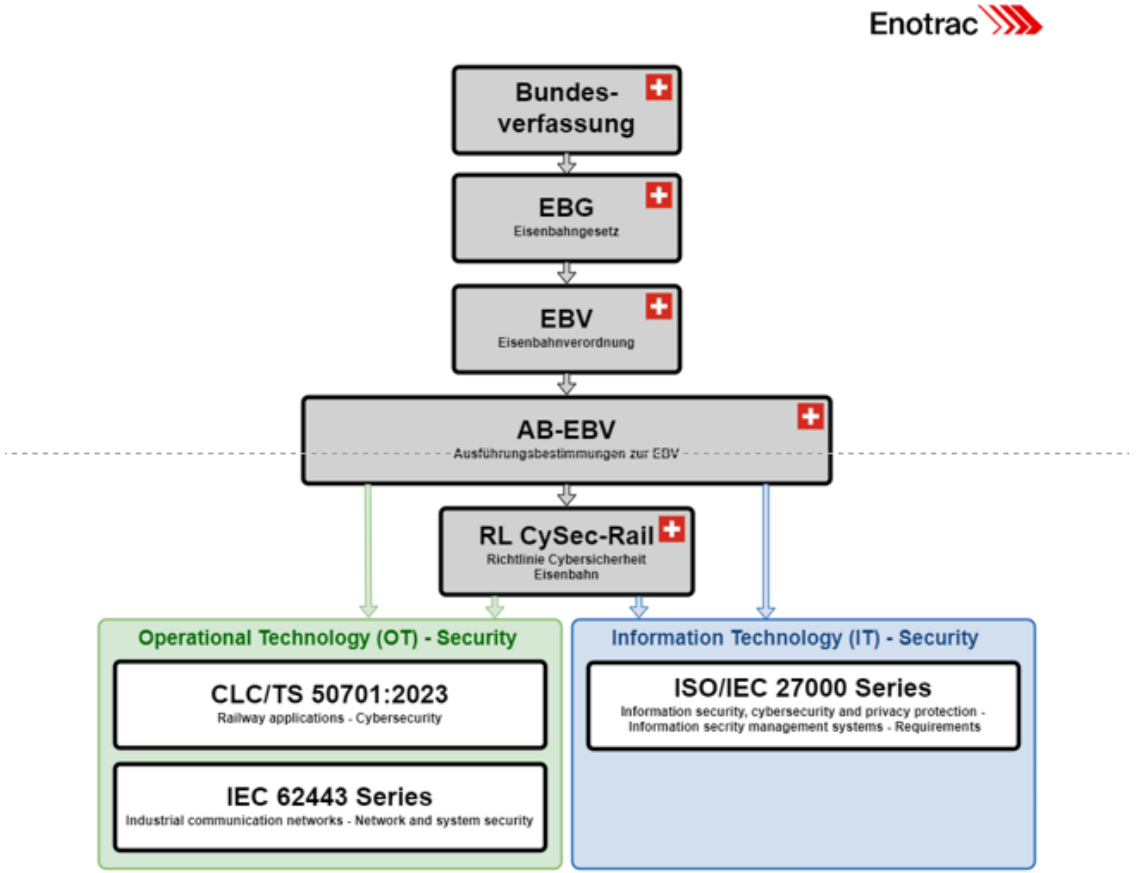
Forschung

SWISSRAIL Industry Association

Arbeitsgruppe Cybersecurity

Kontext

- Richtlinien Cybersecurity Rail des BAV treten am 1. Juli 2024 in Kraft
- Umsetzung steht am Anfang – grosse Unsicherheit
- Hilfestellung durch den Verband



→ **Empfehlungen zur Umsetzung von Cybersecurity**

Positionspapier

- Empfehlungen zur Umsetzung der Basismassnahmen (Kap. 8)
  - IT und OT
- Zielgruppe: Schweizer KMUs, die sich bisher nicht mit Cybersecurity befasst haben
- Zusammenarbeit mit RAILplus
  - Einbezug externer Perspektive
  - Gemeinsame Sprache zwischen Industrie und Betreibern
- Abgleich mit BAV

Nr.	Control	Verweis	Synergie zu VO 2018/762 [3]
B-01	**Festlegung von Rollen und Verantwortlichkeiten** Es müssen Rollen und Verantwortlichkeiten für den Bereich der Informationssicherheit definiert werden. Die einzelnen Aufgabenbereiche müssen Personen mit den entsprechenden Fachkenntnissen zugewiesen werden.	ISO/IEC 27002:2022 Kapitel 5.2 NIST CSF 1.1 ID.GV-2	Kapitel 2.3 Kapitel 4.1 Kapitel 4.2
B-02	**Zugriffs- und Identitätsmanagement** Identitäten von Personen und Systemen, die Zugriff auf Informationen oder anderen Assets haben, müssen verifiziert und verwaltet werden. a) Eine Identität muss immer nur einer Person oder einem System zugeordnet werden. b) Es ist festzulegen, welche Identitäten welche Berechtigungen und Zugriffe erhalten. c) Dabei sind die Grundsätze des "Need-to-know-" und des "Least-privilege-Prinzips" anzuwenden. d) Die vergebenen Berechtigungen müssen regelmässig überprüft und den aktuellen Begebenheiten angepasst werden. e) Nicht mehr aktive Identitäten sind zu deaktivieren.	ISO/IEC 27002:2022 Kapitel 5.3 Kapitel 5.15 Kapitel 5.16 Kapitel 5.17 Kapitel 5.18 NIST CSF 1.1 PR.AC-1 PR.AC-2 PR.AC-4 PR.AC-6	

Weiteres Vorgehen

- Abschluss Positionspapier
- Regelmässiger Erfahrungsaustausch innerhalb der Industrie und mit weiteren Akteuren
- Fokus und Abgleich Europa
- Unterstützung für Initiierung einer Schweizer Meldestelle (Branche)