TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT "IT-Sicherheitsrechtstag 2023"

Berlin, 28.09.2023

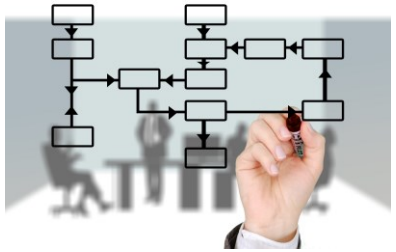
KRITIS-Verordnung vs. Digitalisierung im Bankenumfeld

Touria Jandusch, Commerzbank AG

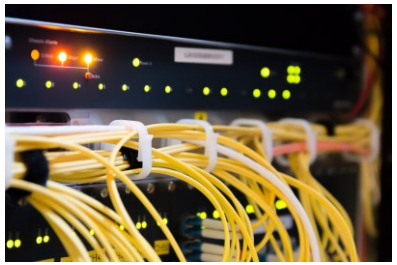
Maschinenraum einer Großbank und die KRITIS-Verordnung

Kritische Infrastrukturen

IT-Produkte „IT-SiG-relevant“



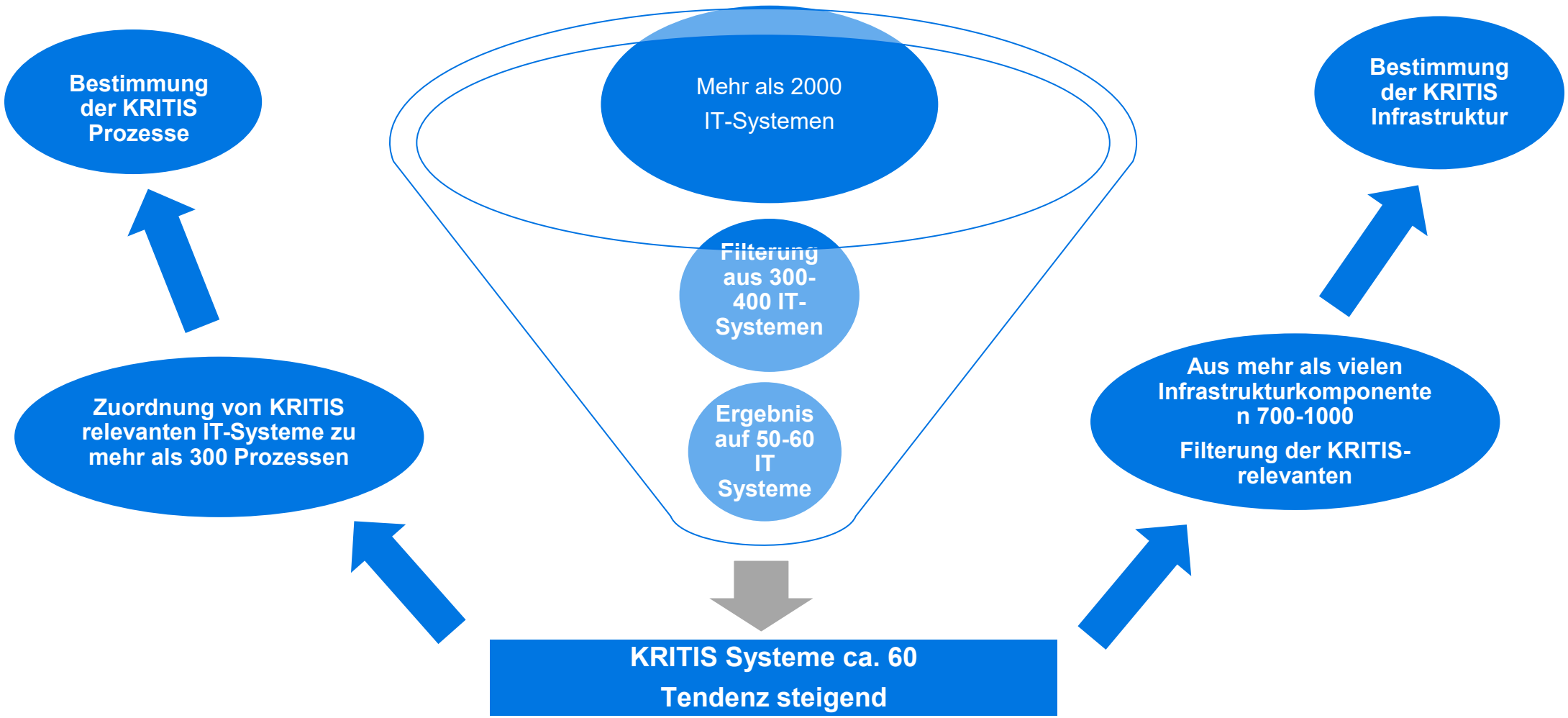
Prozesse und Auslagerungen



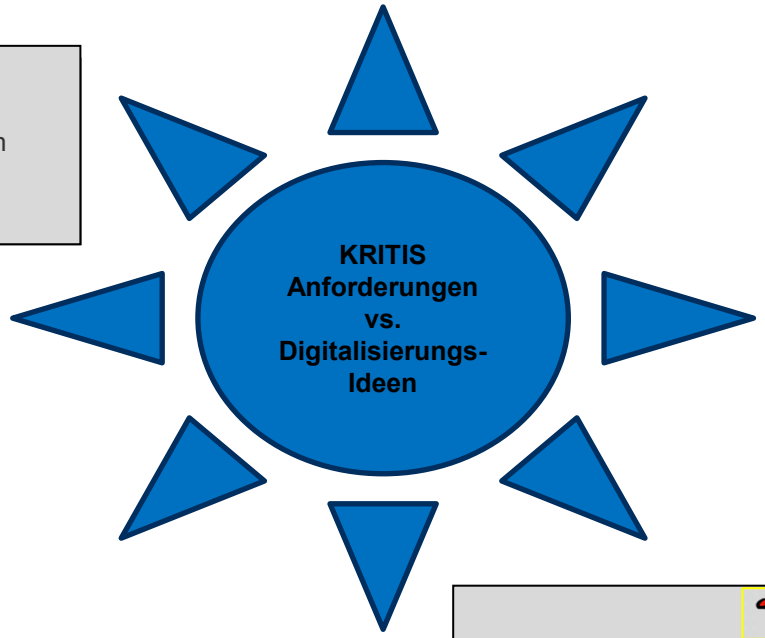
Indirekt unterstützende Systeme & Infrastrukturkomponenten

Rollen, Personen und Organisationseinheiten

Geordnete Analyse oder Suche im Heuhaufen?



Herausforderung in der Umsetzung des IT-Sicherheitsgesetz – Passt Anlage + Schwellenwert zur Digitalisierung?



Große Banken mit über die Jahre gewachsenen Systemen

Sehr heterogene Struktur der Verantwortlichen nicht nur den einen einzelnen Ansprechpartner

Nicht nur das eine Rechenzentrum

Hoher Aufwand durch zu viele unterschiedliche Regularien zum selben Sachverhalt/ IT-Sicherheitsgesetz mit allen anderen Gesetzen

Aufbau ausgewogener Leistungsfähiger Digitalisierungsteams zum Thema Security

Digitalisierung der Systemlandschaft und regulatorische Anforderung nicht immer kompatible

Fragilität bei Veränderungen, da sehr starke Vernetzungen der Systeme z.B. Kennzeichnung Schlüsselinfrastrukturen

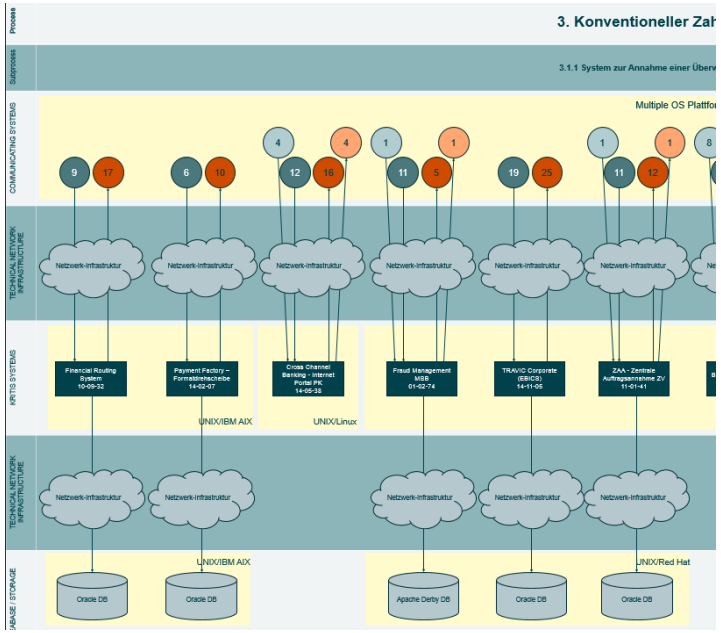
Silos / Kulturunterschiede bzgl. Des Verständnis für Security

Klassisch oder Agil, welche Wege führen zur Umsetzung der KRITIS-V im Bankenumfeld?

- **Wie ist die Sichtbarkeit des Themas IT-Sicherheit, bei Digitalisierungsprojekten?**
  Standardisierung von Anforderungslisten, die ein Jeder vor dem Digitalisierungsprojekt Start kennen muss.
- **Welche Form der Gespräche sollen mit den Schnittstellen und anderen Beteiligten geführt werden, um sie auch von der Beteiligung an der Umsetzung zu überzeugen?**
  Adressatengerechte Gespräche mit Unterstützungsleistung in der Umsetzung: z.B. „welche Assets habe ich im KRITIS Prozess?“ und „Was muss ich erfüllen?“
- **Nur interne oder auch Externe Beteiligte?**
  Interne Verantwortliche aufklären, diese kommen Ihrer Verantwortung nach, die Dienstleister aufzuklären z.B. kümmert sich die Retained Organasition, um das KRITIS Verständnis beim jeweiligen Dienstleister und prüft die Richtigkeit der Vereinbarungen und verhandelt Ergänzungsverträge zur Erfüllung der KRITIS-V-
- **Wie soll das Management unterstützen?**
  Management muss einbezogen werden, da diese als dezentrale Risikomanager:Innen die Entscheidungsträger:Innen sind.
- **Weiß Jeder in der Bank, welche Pflichten damit verbunden sind und um das Risiko der kritischen Infrastruktur im Sinne KRITIS?**
  Aufklärung durch verschiedene Kommunikationswege z.B. auch über spezifische Vernetzung durch die Communities, Schulungen und der Einbeziehung der 2nd Line (Standardsetzer) bei der Planung von Projekten.
- **Wieviel Digitalisierung verträgt KRITIS und ist es möglich?**
  Standards können im KRITIS-Prozess digitalisiert werden z.B. das zusammentragen von Daten, die Prüfung der KRITIS Relevanz ist in großen Banken ohne manuellen Aufwand bei heterogene Landschaft nicht einfach. Vorgaben sind zu eng gefasst.

Von Analog zu Digital in der Netzlandschaft einer Großbank

Manuell erstellter Plan



Schnittstellen der KRITIS Systeme im Kartengestützten Zahlungsverkehr inkl. Verbindungen zu externen Partnern*

Digitalisierung mit Echtzeitdaten

Eventgetriebene Wertpapierabwicklung - Kapitalmaßnahmen

Eventgetriebene Wertpapierabwicklung - Kapitalmaßnahmen Network

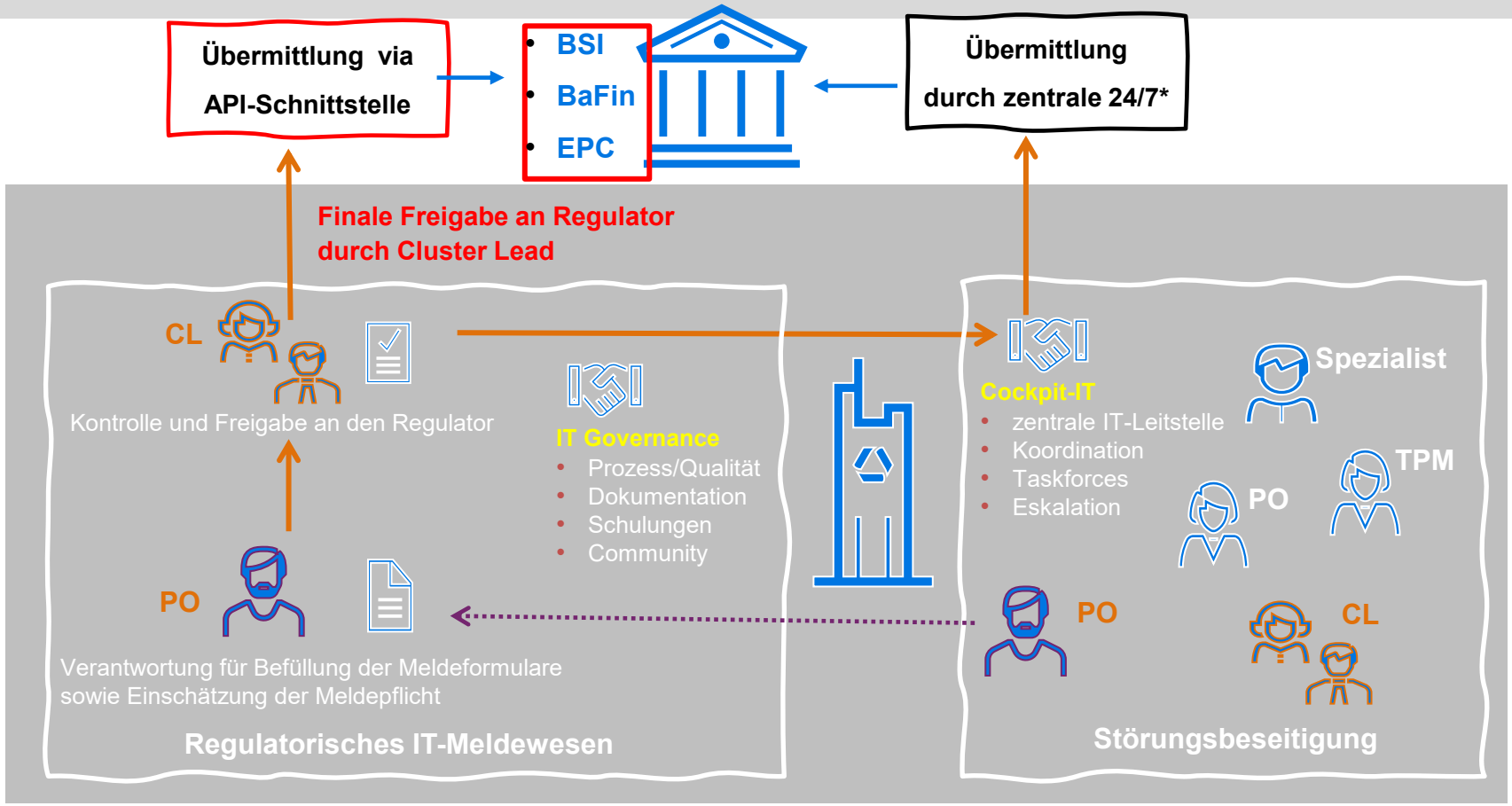
Eventgetriebene Wertpapierabwicklung - Kapitalmaßnahmen: Incoming Interfaces

		metric	COUNT(*)	
		source_application_operation	Extern gehosted	Intern
target_product_id	target_product_name			
06-01-14	WP-Abrechnung			54
06-01-26	Straight Through Processing (STP) - Wertpapier			39
06-02-01	WP-Stamm- und Termindaten (wst)			12
06-02-05	Depotbuchung			129
14-02-36	NGFM Traffic Services		2	1

Eventgetriebene Wertpapierabv

source_product_id	source_product_na
06-01-14	WP-Abrechnung
06-01-26	Straight Through P
06-02-01	WP-Stamm- und T
06-02-05	Depotbuchung
14-02-36	NGFM Traffic Servi

IT-Meldewesen: Von Analog zu Digital wo sind die Barrieren einer Großbank?



Die Verantwortung der regulatorischen Meldungen liegt im jeweiligen Cluster

Das IT-Sicherheitsgesetz kann Motor für Awareness der Security Governance sein

Kontinuierliche Verbesserung durch wiederkehrendes überprüfen und steuern auf allen Ebenen im und um Die Vorgaben zum IT-Sicherheitsgesetz, kann die Erfüllung von regulatorischen Anforderungen und die Verbesserung der Prävention von Risiken für Banken erleichtern