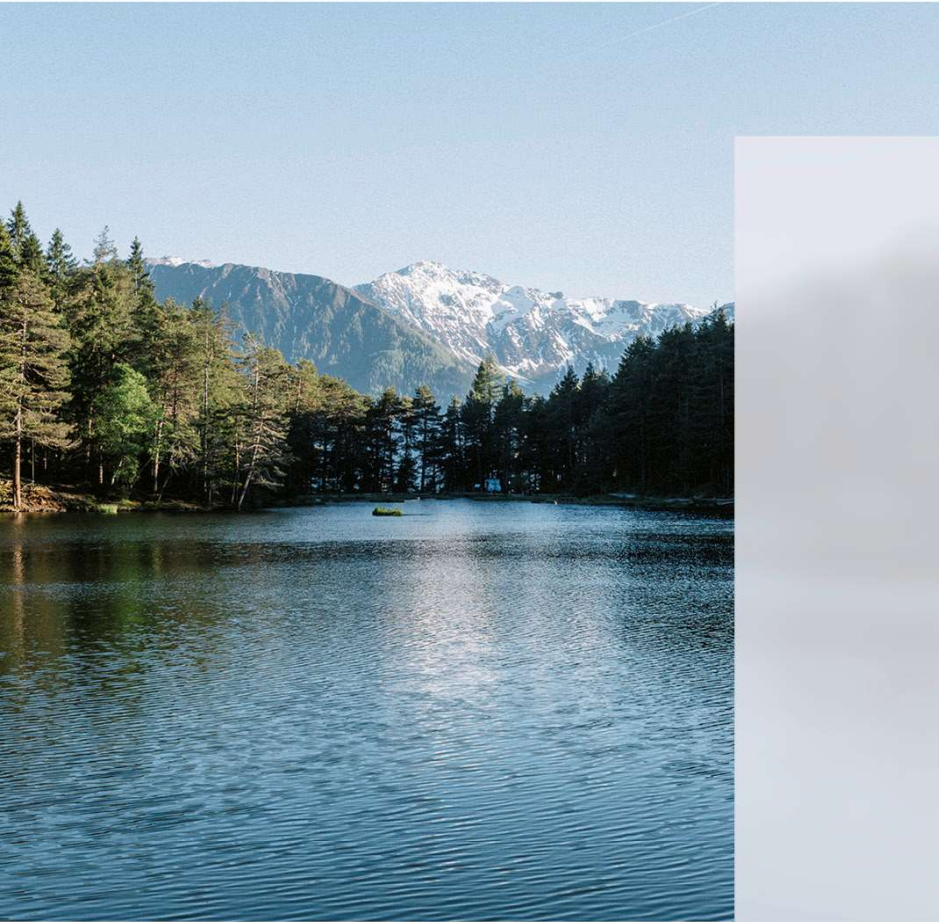




Resilienzmanagement

Von der **digitalen** Resilienz gemäß
der DORA-VO (EU) zur integrierten
operationellen Resilienz im
Banksektor

IKT-Sicherheitskonferenz – Dornbirn, am 25.06.2025

Referent **Philipp Ladurner**

Berufserfahrung

- 15 Jahre FüU-Bereich Österreichisches Bundesheer
- 2 Jahre IT-Risikomanagement Bankenrechenzentrum
- 2,5 Jahre Business Continuity-, Notfall- und Krisenmanagement Hypo Tirol Bank



Ausbildung

- Stabsunteroffizierslehrgang
HUAK – Heeresunteroffiziersakademie
- BSc „Integriertes Sicherheitsmanagement“
FH Campus Wien
- MA „Risiko- und Compliancemanagement“
TH Deggendorf

Agenda

- Prinzipien der operationellen Resilienz
- DORA – Digital Operational Resilience Act
- Von der digitalen Resilienz zur integrierten operationellen Resilienz
- Von der Compliance zur strategischen Stärke

Prinzipien der operationellen Resilienz

(BCBS 2021 – Basel Committee on Banking Supervision)

Operationelle Resilienz wird als Fähigkeit der Bank definiert, **kritische Geschäftsabläufe** auch bei Störungen aufrechtzuerhalten. Diese Fähigkeit versetzt eine Bank in die Lage, Bedrohungen und potenzielle Ausfälle zu erkennen, sich davor zu schützen, angemessen darauf zu reagieren und sich anzupassen sowie sich von ihnen zu erholen und aus ihnen zu lernen.

Operationelle Resilienz ist ein Ergebnis, das vom **effektiven und effizienten** Management operationeller Risiken profitiert.

Dazu zählen:

- Risikoidentifikation, -analyse und -bewertung
- Risikominderung (einschließlich der Implementierung von Kontrollen)
- Überwachung von Risiken und Kontrolleffektivität
- Fähigkeit, auf Störungen zu reagieren und sich davon zu erholen

Prinzipien der operationellen Resilienz

(BCBS 2021 – Basel Committee on Banking Supervision)

Weitere **wichtige Faktoren:**

- Three Lines of Defence
- Geschäftsfortführung
- Outsourcing von Dienstleistungen
- Wiederherstellungs- und Abwicklungsplanung

Nur eine kollektive Betrachtung und die Integration der Managementsysteme führt zur
operationellen Resilienz

DORA – Digital Operational Resilience Act

DORA-VO: DeVO (EU) 2022/2554

- Inkrafttreten 16.01.2023
- Ende Übergangsfrist zur Umsetzung 17.01.2025

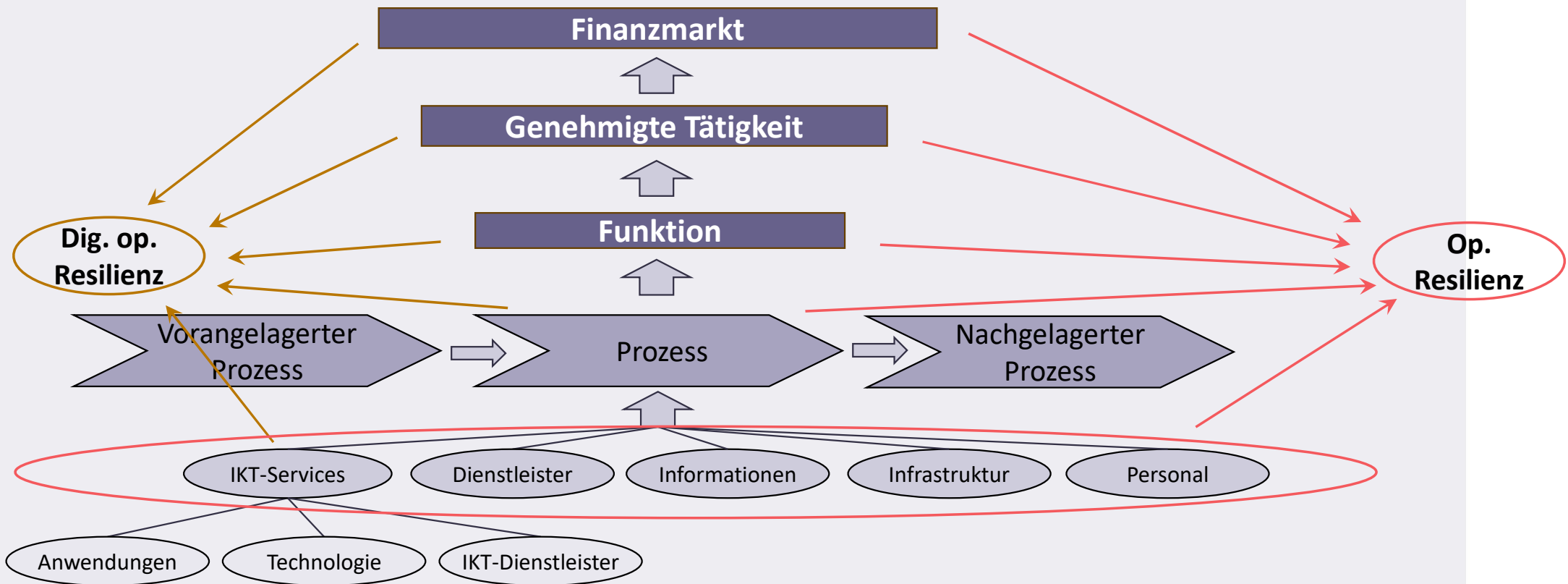
Ziel:

- Harmonisierung diverser regulatorischer Anforderungen bezüglich IKT

Fokus:

- IKT-Risikomanagement
- IKT-bezogene Vorfälle
- Testen der digitalen operationellen Resilienz
- Management des IKT-Drittparteienrisikos
- Überwachungsrahmen kritischer IKT-Drittdienstleister
- Informationsaustausch und Notfallübungen

Von der digitalen Resilienz zur integrierten operationellen Resilienz



Von der Compliance zur strategischen Stärke

Kontext der Organisation

- **Who am I?**

Stakeholder Anforderungen

- **What am I supposed to do?**

Umsetzung

- **What do I need to do to fulfill my primary business purpose?**

➤ Implementierung der Managementsysteme

- **Governancemanagementsysteme**
- **Risikomanagementsysteme**
- **Compliancemanagementsysteme**

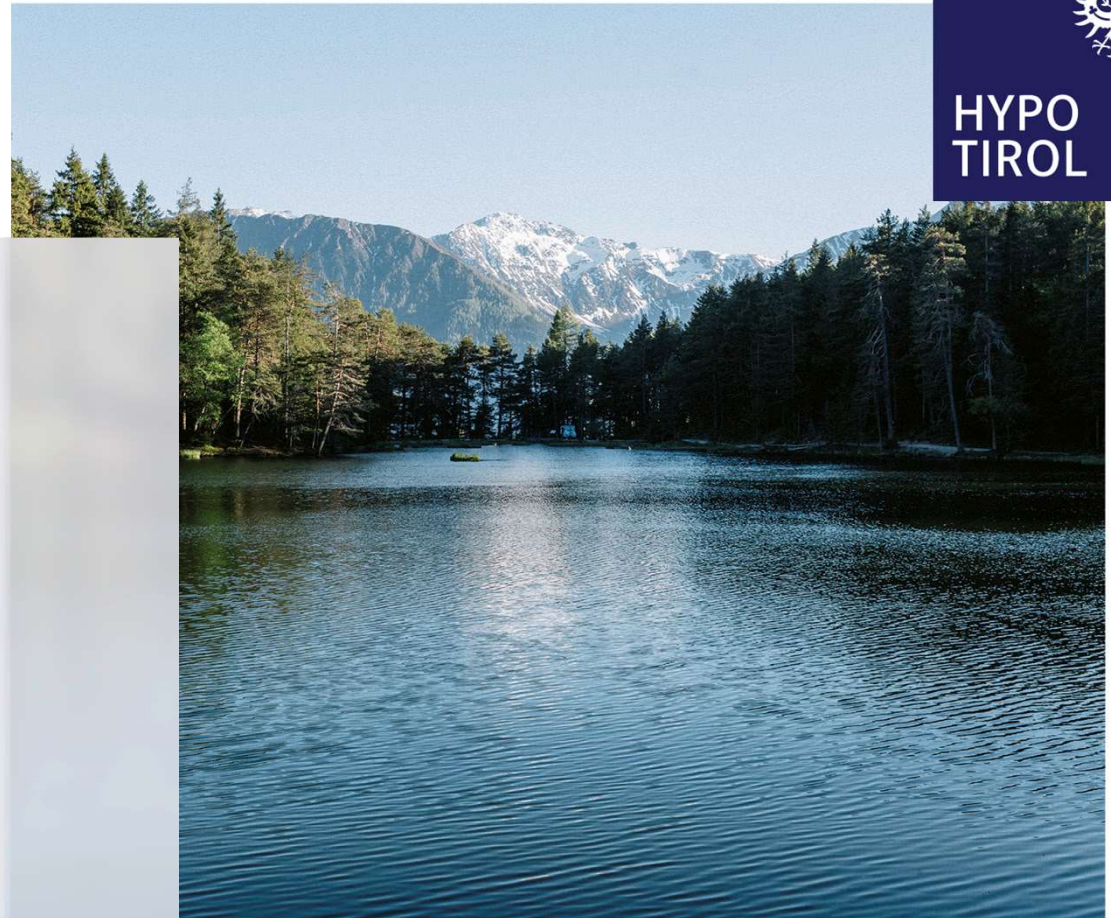
➤ Integration der Managementsystemen

- **Gemeinsame Definitionen**
- **Synergetische Methoden, Analysen, Prozesse und Zyklen**
- **Gesamtrisikosteuerung**

Von der Compliance zur strategischen Stärke

- Effektiver Ressourceneinsatz
- Wirtschaftliche Arbeitsweise
- Klare Priorisierung
- Produktsicherheit
- Rechtliche Sicherheit
- Managen von disruptiven Ereignissen
- Resiliente Organisation
- Wettbewerbsvorteil

Fragen



DANKE für die
Aufmerksamkeit



HYPO
TIROL