INNOQ TECHNOLOGY DAY / 13.11.2023

Compliance in hybriden Betriebsumgebungen

Eine soziotechnische Betrachtung

INNOQ

ANJA KAMMER
SENIOR CONSULTANT

Agenda

Compliance in der Praxis

Niemand hat Bock darauf

Hybride Betriebsumgebungen

Typische Herausforderungen

Soziotechnische Maßnahmen

Für soziotechnische Probleme

Fazit

Compliance in der Praxis

Niemand hat Bock darauf

ZEIT ONLINE

IT-Sicherheit in Gesundheitsämtern

Alle kennen die Sicherheitslücken und keiner schließt sie

In Rheinland-Pfalz setzen Gesundheitsämter eine veraltete Software voller Sicherheitsprobleme ein. Doch die Lücken werden lieber wegdiskutiert, statt geschlossen.

Von **Kai Biermann** und **Eva Wolfangel**

10. November 2023, 16:03 Uhr / 80 Kommentare /

Kai Biermann, Eva Wolfangel. (2023). IT-Sicherheit in Gesundheitsämtern: Alle kennen die Sicherheitslücken und keiner schließt sie. Retrieved from https://www.zeit.de/digital/datenschutz/2023-11/it-sicherheit-gesundheitsaemter-rheinland-pfalz-software-datenschutz

“Regulierungstsunami - schwer ***alles im Blick*** zu behalten und in den richtigen Kontext zu stellen.”

"Sicherheit und Konformität stehen oft im ***Widerspruch***."

"Feedback zur Umsetzung von Vorgaben fehlt. Entwicklungsteams werden ***allein gelassen***."

"Möglichst restriktive Auslegung implementieren, um ***auf der sicheren Seite*** zu sein."

"Fehlannahme: Betrieb On-Premises ist ***automatisch sicher und konform***."

"Ignoranz mit voller Absicht, wenn man ***nicht zu den großen Fischen gehört***."

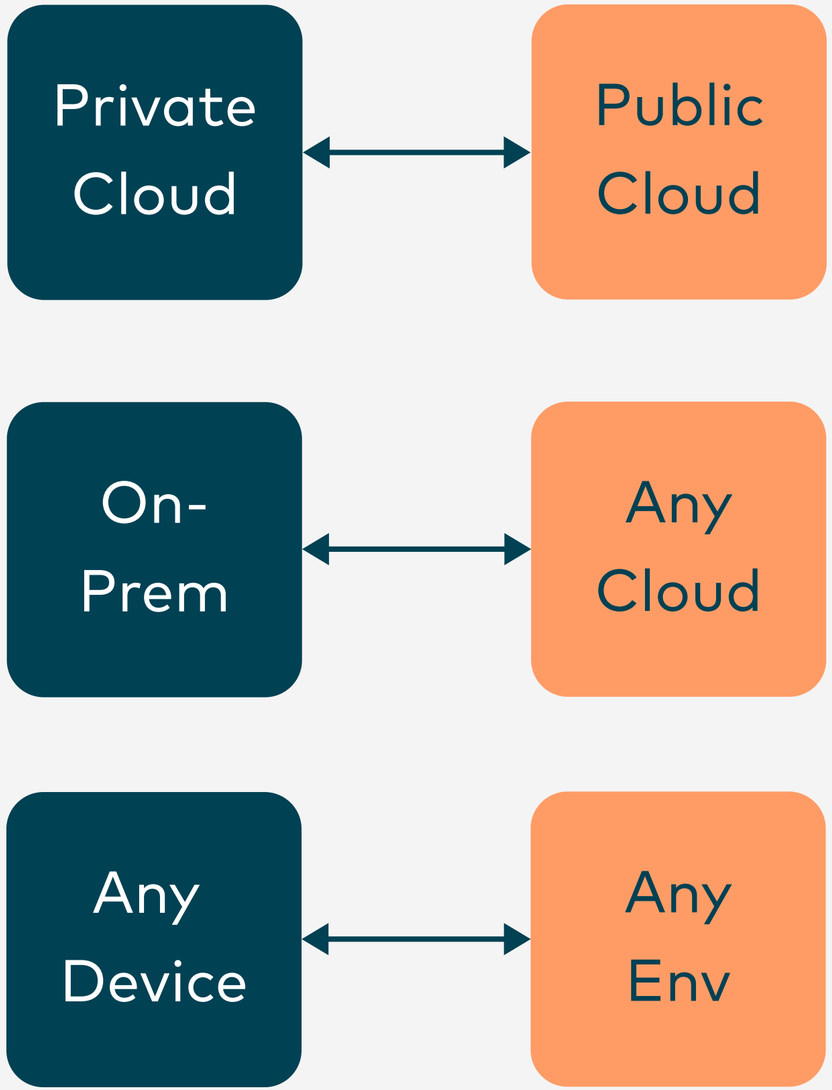
Hybride Betriebsumgebungen

Typische Herausforderungen

Hybride Betriebsumgebungen

Gesamtsystem, das voneinander abhängt

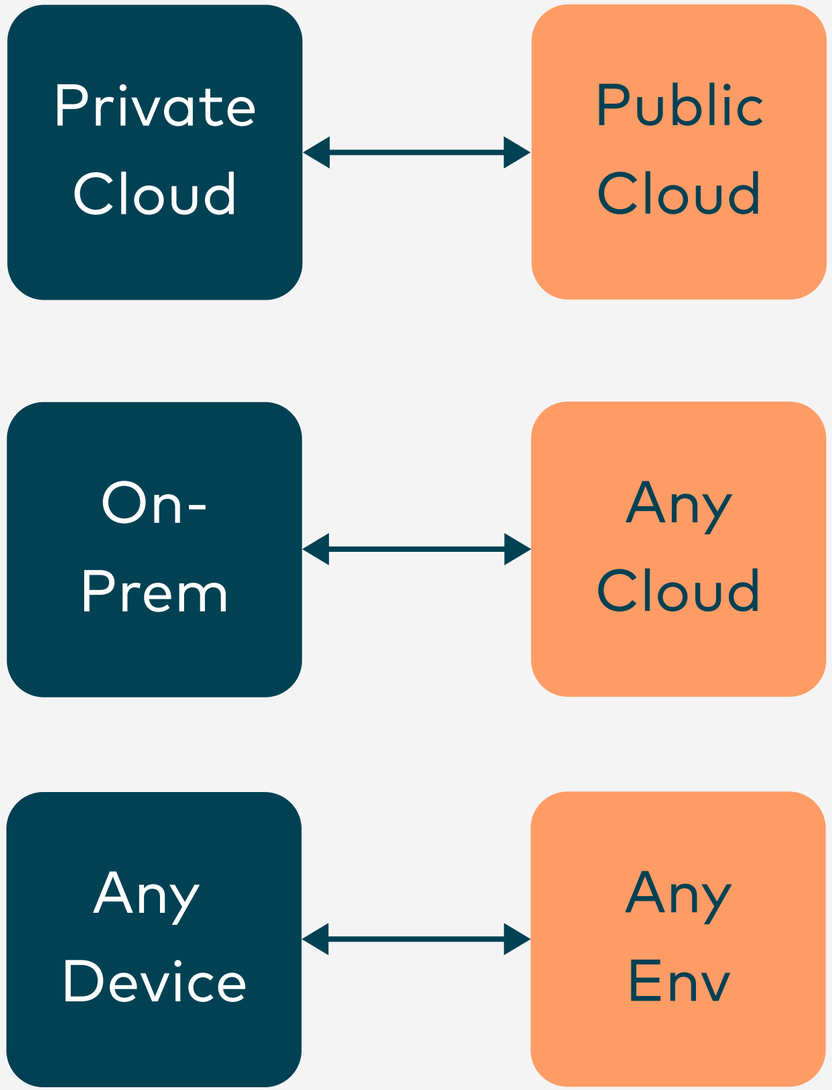
- Hybrid-Cloud (Private + Public)
- On-Premises + Cloud
- IoT + (?)
- Mobile + (?)



Vorteile hybrider Betriebsumgebungen

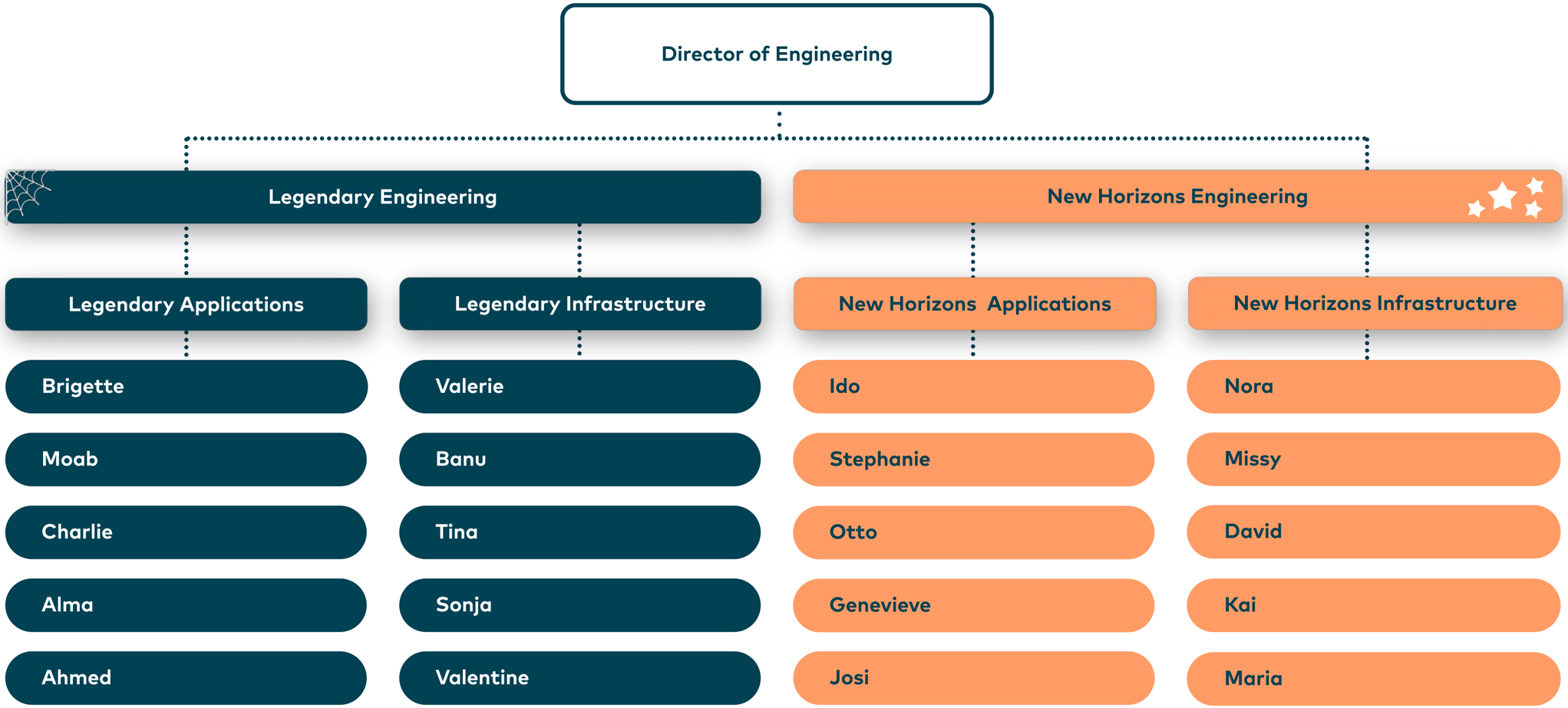
Vorteile

- (IoT/Mobile) Bestandteil der Architektur
- Lastspitzen ausgleichen
- Schrittweise Migration
- Kritische Systeme bleiben On-Prem



Herausforderungen hybrider Betriebsumgebungen

- Abstimmung von Compliance-Maßnahmen
- Umsetzung und Überwachung geltender und zukünftiger Compliance-Vorgaben
- Sicherstellung von Datenintegrität und -sicherheit bei Transfer
- Fortlaufende Verwaltung von Zugriffsberechtigungen


Director of Engineering
Legendary Engineering
New Horizons Engineering
Legendary Applications
Legendary Infrastructure
New Horizons Applications
New Horizons Infrastructure
Brigette
Moab
Charlie
Alma
Ahmed
Valerie
Banu
Tina
Sonja
Valentine
Ido
Stephanie
Otto
Genevieve
Josi
Nora
Missy
David
Kai
Maria

Soziotechnische Maßnahmen
Für soziotechnische Probleme

Föderale Compliance-Gruppe

What Is Data Mesh?

	Domain Ownership	Data as a Product	Self-serve Data Platform	Federated Governance
Strategic Domain-driven Design	Domain Bounded Context	Product Thinking	Domain-agnostic	Context Mapping
Socio-technical Perspective	Domain Teams	Data Product by Domain Team	Data Platform Team	Governance Group
Technology	Operational & Analytical Data	Interoperability Interfaces	Self-serve Data Platform	Policy Automation

datamesh-architecture.com

Data Mesh Governance

Members

Domain Teams Representatives

Data Platform Team Representatives

Subject Matter Experts (legal, privacy, ...) on demand

Global Policies

Context
The issue at hand, goal, situation., former decisions. Why are we talking?

Decision
The agreed decision.

Consequences
Effects, outcomes, costs, follow-up questions.

Policy Automation

Policy as Code
How to automate a policy by the data platform?

Automated Tests
Data quality checks in CI/CD-Pipelines

Monitoring
Compliance and drift detection

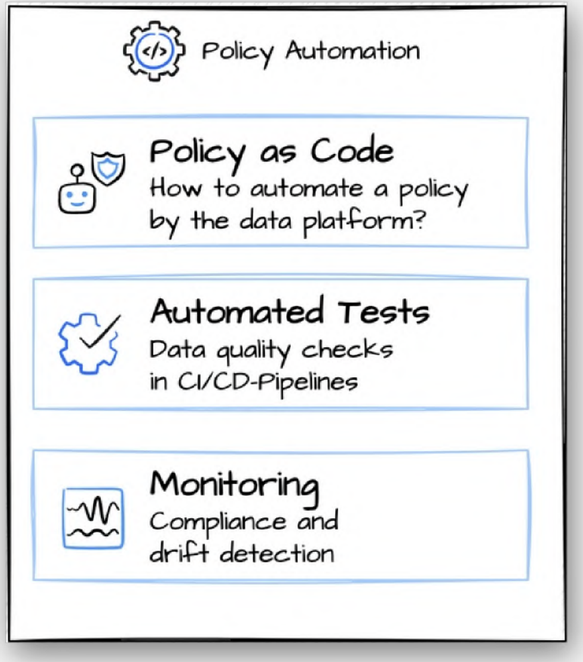
Federated Governance

datamesh-governance.com

Automatisiertes Policy-Management

Automatisiertes Policy-Management

- Policy as Code
- Automatisiertes 'Policy Enforcement'
- Überwachung (Auditing)



datamesh-governance.com

Einheitliche Software Delivery Prozesse

Self-Service Plattform

Plattform Engineering

konforme
Plattform-Services

Einheitliches
Setup

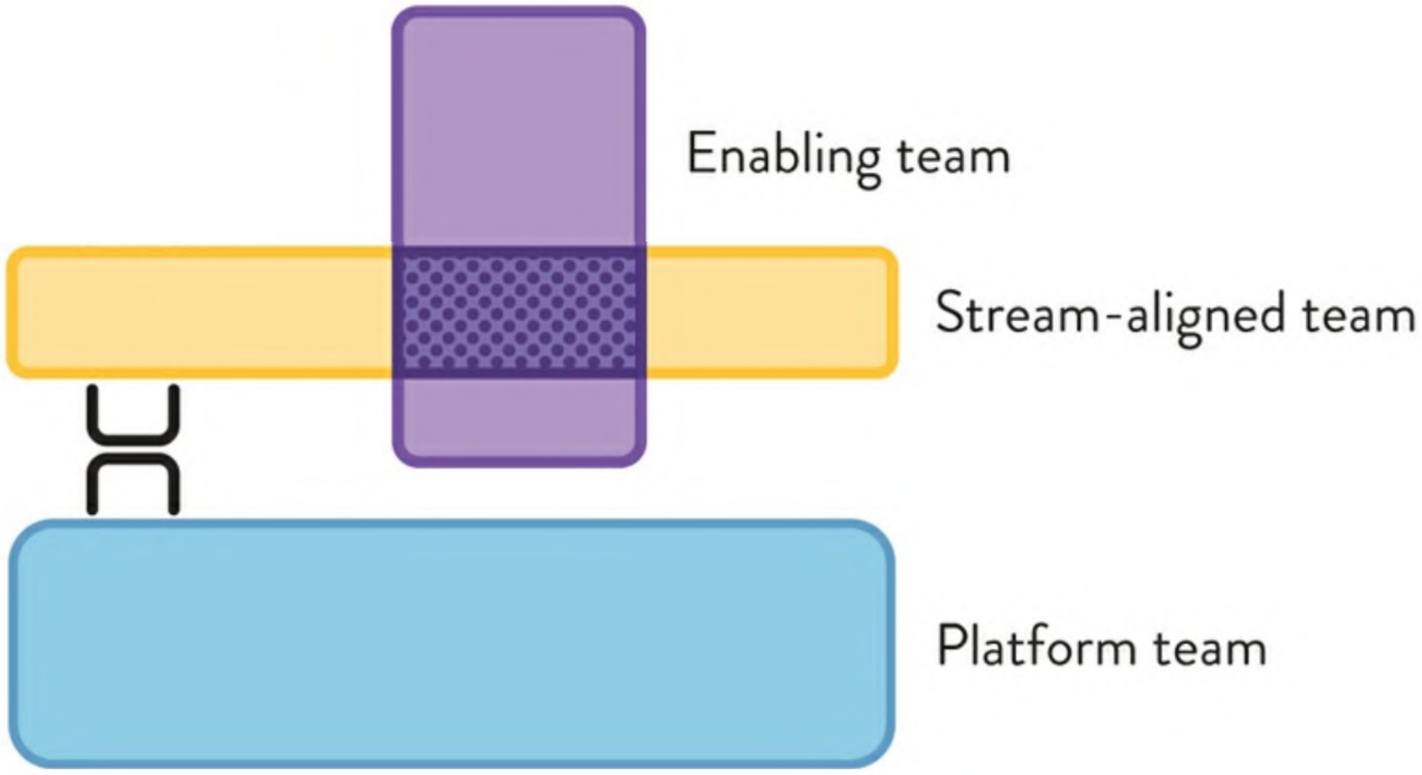
Infrastruktur
on-Demand

Policy
Enforcement

Dedizierter Support

Unterstützende

Teams



Team Topologies. Organizing Business and Technology Teams for fast Flow. Matthew Skelton, Manuel Pais. (2019). p. 80

Pioneer-Teams

Fazit

Compliance ist kein bürokratischer Selbstzweck

Soziotechnische Maßnahmen

Föderale Compliance-Gruppe

Gebündelte Expertise und Wissensverteilung

Automatisiertes Policy-Management

Erleichterte Durchsetzung und Überwachung

Einheitliche Software Delivery Prozesse

Entlastung und Überwachung globaler Policies

Self-Service Plattform

'Compliant by Default' als internes Produkt

Dedizierter Support

Unterstützung bei der Umsetzung

Pioneer-Teams

Bedarfsgerechte Umsetzung zentraler Services

Danksagung

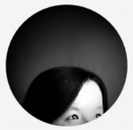
INNOQ
www.innoq.com

Christoph Iserlohn

Daniel Lauxtermann

Jakob Oswald

Jerry Preissler



Martina Meng

Theo Pack

innoQ Deutschland GmbH

Krischerstr. 100
40789 Monheim
+49 2173 333660

Ohlauer Str. 43
10999 Berlin

Ludwigstr. 180E
63067 Offenbach

Kreuzstr. 16
80331 München

Hermannstr. 13
20095 Hamburg

Erftstr. 15-17
50672 Köln

Königstorgraben 11
90402 Nürnberg