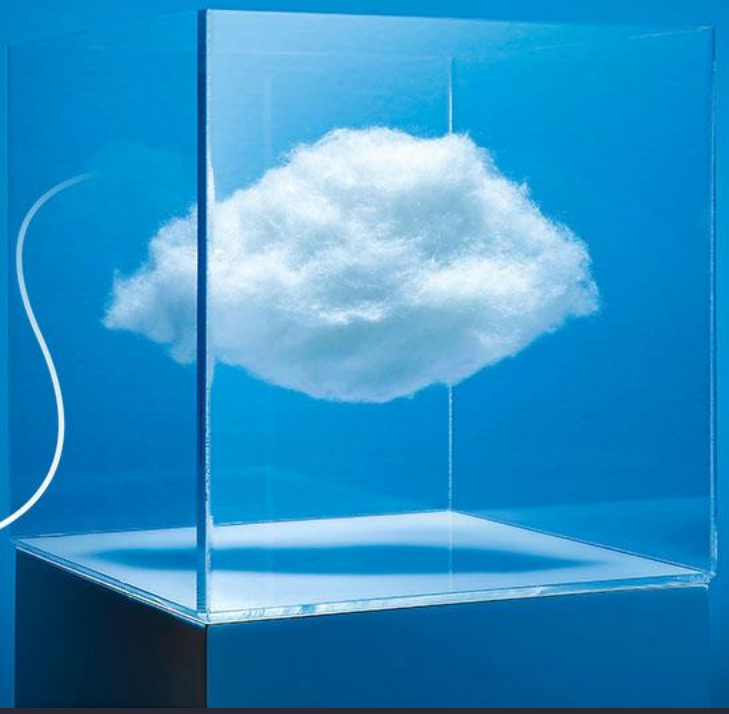
Capgemini

Securing *Sovereignty*

An exclusive Capgemini event on Sovereign Cloud

Oct 10th | 12:00 - 17:30 | InnStyle, Maarssen



In collaboration with: Microsoft | Google | aws

Agenda

12:00	Welcome and lunch
13:00	Opening
13:15	Impact of cyber threats, geopolitical tensions and stricter laws & regulations on cloud adoption
14:00	Developments and applications of sovereign cloud solutions
14:45	Break
15:15	Session 1 (Vision Cloud Service Providers on Sovereign Cloud)
16:15	Session 2 (Vision Cloud Service Providers on Sovereign Cloud)
17:00	Closing, nibbles and drinks

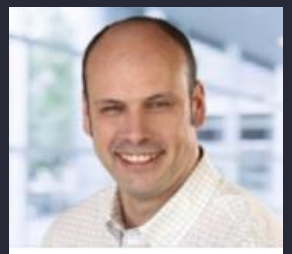
Our Speakers today

Ronald Walthaus

Cloud Lead, Capgemini

Michael Stoelinga

Principal Consultant / Public Sector, Capgemini



Sefan Zosel

Cloud Lead Global Public Sector / Sovereign Cloud, Capgemini

Michiel van Otegem

Cloud Sovereignty Architect / Global Engineering, Microsoft

Julien Blanchez

Digital Sovereignty Solution Lead, Google

Alex Meek Holmes

Global Business Development - Sovereignty and Infrastructure, AWS

Our household rules for today

- We would like to follow the Chatham House Rules.
- Be careful in case posting something on Social Media, do not quote any companies – or people. So, people can speak freely.
- Please go after the 1st breakout directly to the 2nd one.

Feedback

- We would appreciate if you can fill in our feedback form after the sessions

Capgemini Research

Elements of cloud sovereignty

Data Sovereignty		Operational Sovereignty		Technical Sovereignty
• Data Localization: Hosting, using, storing or processing of cloud data in preferred location or jurisdiction (usually home country/ region/territory) • Data Ownership: Data is at all times under the control and ownership of its originator/ producer	• Data Traceability: Focus on management and transparency of data across the lifecycle • Data Access Controls: It is about who can access the data, from where and for what purpose	• Operational Resilience: Ensuring continuity of cloud service in case of unplanned disruptions • Regulatory Compliance: Focus on alignment with region/ sector-specific regulations and laws	• Sovereignty of ecosystem of partners including telcos/ network provider or API calls • Following the security objectives, controls, governance management; detection of and reaction to cyber attacks	• Portability and Reversibility: Ability to move applications and data from one cloud-computing environment to another with minimal disruption • Interoperability: Solution follows integration standards and can be easily connected to existing and/or future solutions from other providers

Note: There is no single definition of cloud sovereignty; the report outlines key elements in Capgemini's views along with the priorities highlighted by organizations.
Source: Capgemini Research Institute Analysis.

Impact of cyber threats, geopolitical tensions and stricter laws & regulations on cloud adoption

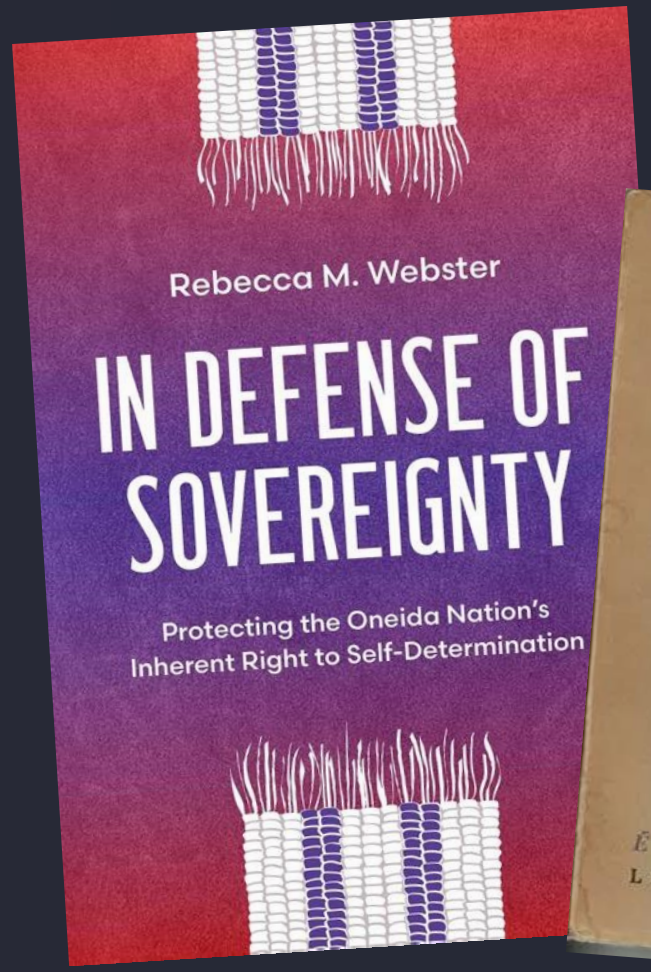
Ronald Walthaus
Cloud Lead,
Capgemini

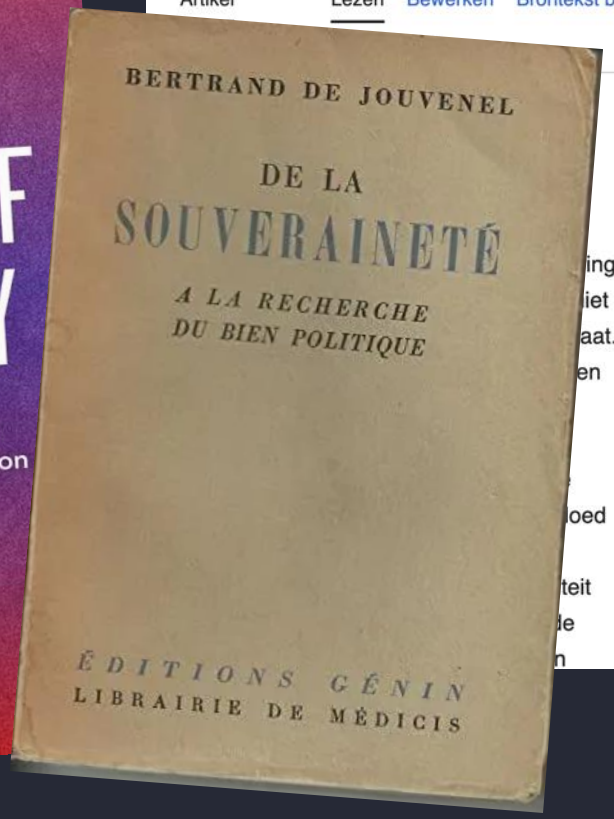
Michael Stoelinga
Principal Consultant / Public Sector, Capgemini

Capgemini

Sovereignty…

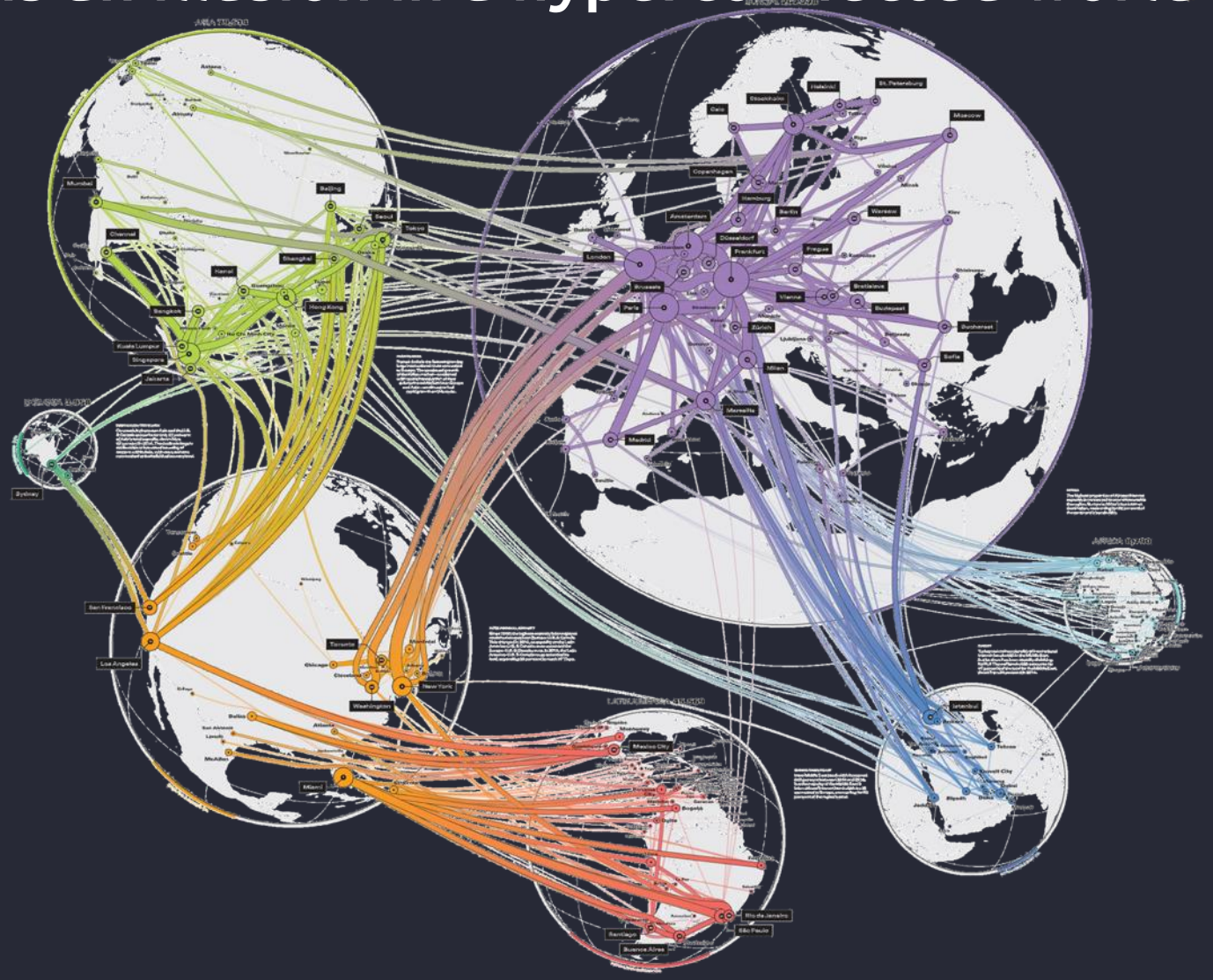
Michael Stoelinga
Chief Architect Public Sector



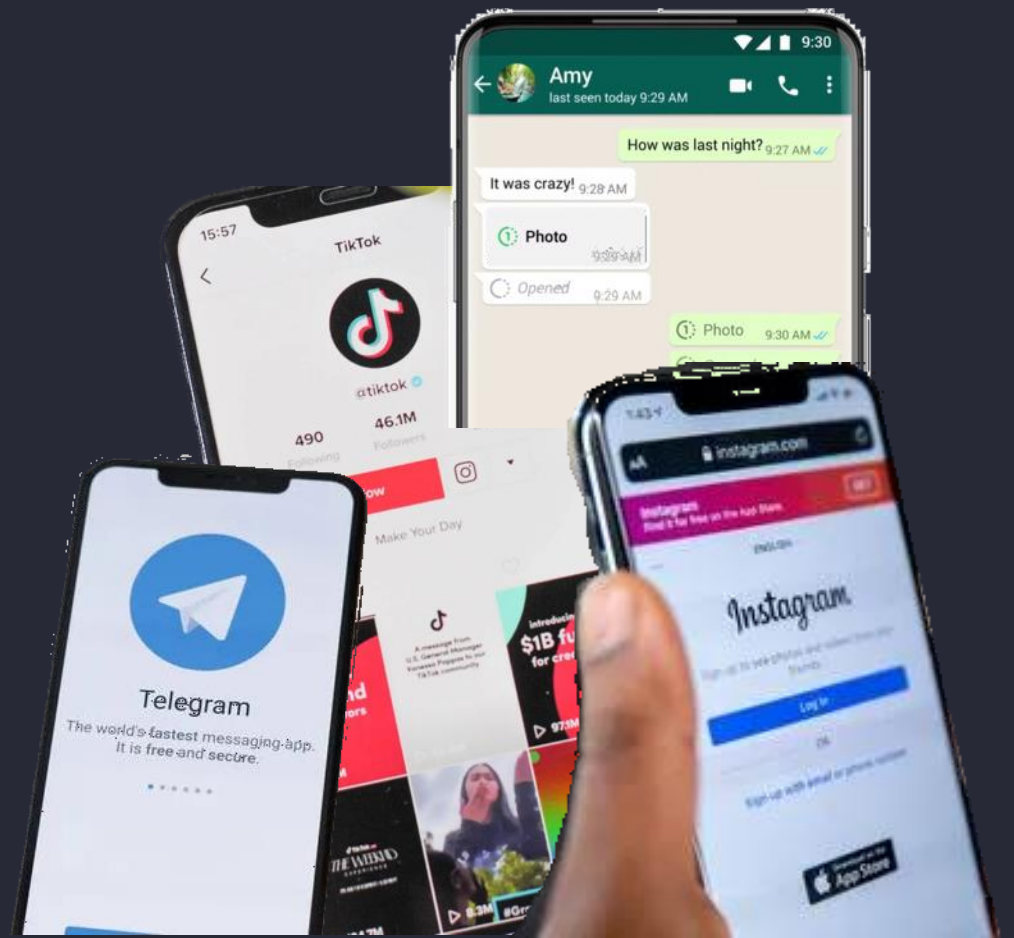


Capgemini

Sovereignty… is an illusion in a hyperconnected world



Private vs. Corporate & Public



Taking responsibility & ownership

- **Different laws & regulations**
- **Contracts**
- **Security**
- **“Unreliability”**
- **Portability**
- **Encryption**
- **Your own keys**
- **Data classification**
- ***Sound advice & expertise***

Cloud is … quite some work…

Your business, societal task is worth it!

CLOUD act perception – saying a risk is low is a communication risk

Vendor lock-in at hyperscaler can be problematic, but the CLOUD act is the wrong reason

NCSC publication:

US CLOUD act is not the only law which reaches beyond the legal territory of a country

As it effects the whole supply chain, an EU based organization could also be targeted

It has not happened until now;

Contract governs GDPR rules for employee data

Use as a citizen is not covered

Much bigger risks:

- Request a person, either a US national working in a EU firm or someone else
- Hack it, hack someone's device
- Complot theories… like state actors have backdoors anyway…

Mitigation:

- High quality encryption
- Providers without access to the keys
- Strict access policies of your personnel
- Monitoring

All of the above are more relevant than whether the jurisdiction of the provider is in EU or US.

Legislation on Cloud

Ronald Walthaus
Cloud Business Transformation Lead

BIO | Baseline Informatiebeveiliging Overheid

CAIQ

Capgemini

Sovereign cloud adheres to the highest level of exclusivity towards control, security and access

CLOUD TYPES COMPARED BASED ON CONTROL, SECURITY AND ACCESS

Level of Cloud Sovereignty

PUBLIC CLOUD

Public Cloud is available to the general public and provided by commercial cloud provider

SECURE CLOUD

Secure Cloud offers enhanced security for a specific organisation and can be either provided by a cloud provider or be private

SOVEREIGN CLOUD

Sovereign Cloud is data and services run from and held within a country (or within EU) complying with local laws & regulations

Cloud sovereignty helps mitigate risks that occur when utilizing cloud services outside the operational territory

RISK EXAMPLES DRIVING THE SOVEREIGNTY DISCUSSION

Image / reputational risk

Legal risk
Contracts and international laws

Security Risk
Network and supply chain effect

A market dominated by a small number cloud providers

Insufficient visibility and control over what is being done on customer data

Relatively opaque location and exposure to extraterritorial laws

Dependence on suppliers based in non-EU jurisdictions

No direct control over the physical access infrastructure

Economic risk
Low competition and data leakage

Operational Risk
Service access restrictions

KEY DIFFERENTIATORS OF A SOVEREIGN CLOUD

Localisation

Physical Locations

Enhanced Security

Governance

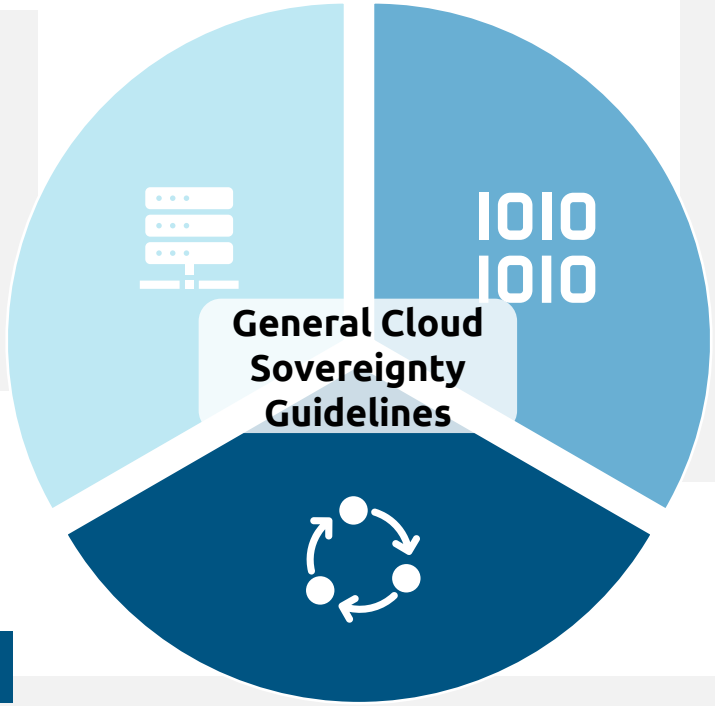
Compliance

We assess cloud sovereignty from 3 dimensions to consider technical, data and operational aspects

Technical Sovereignty

1- Reversibility & Portability

2- Interoperability



Data Sovereignty

3- Localization

4- Ownership

5- Access management

6- Transparency

Operational Sovereignty

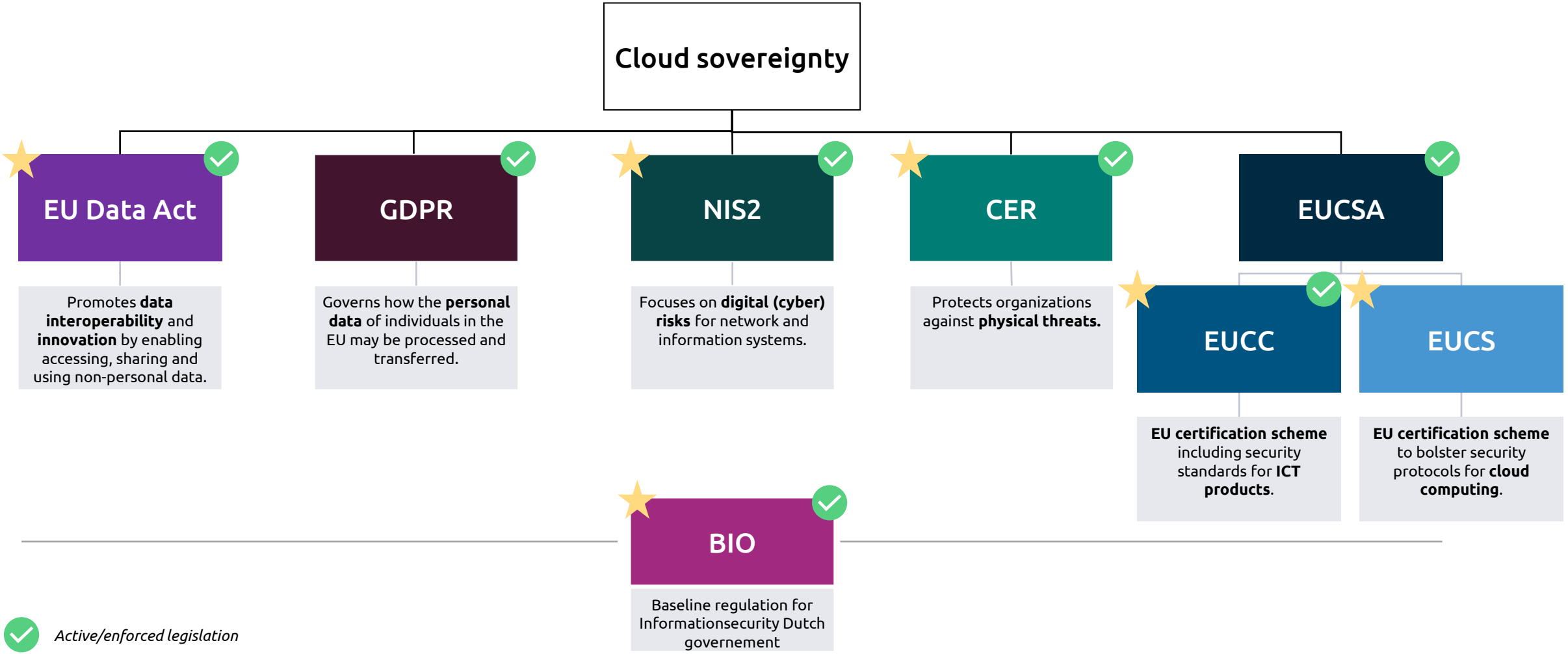
7- Operational resilience

8- Regulatory and Compliance

9- Sovereignty of ecosystem of partners

10- Following the security

Cloud Sovereignty is linked to legislation such as the EU Data Act, GDPR, NIS2, CER, and the EU-cyber schemes



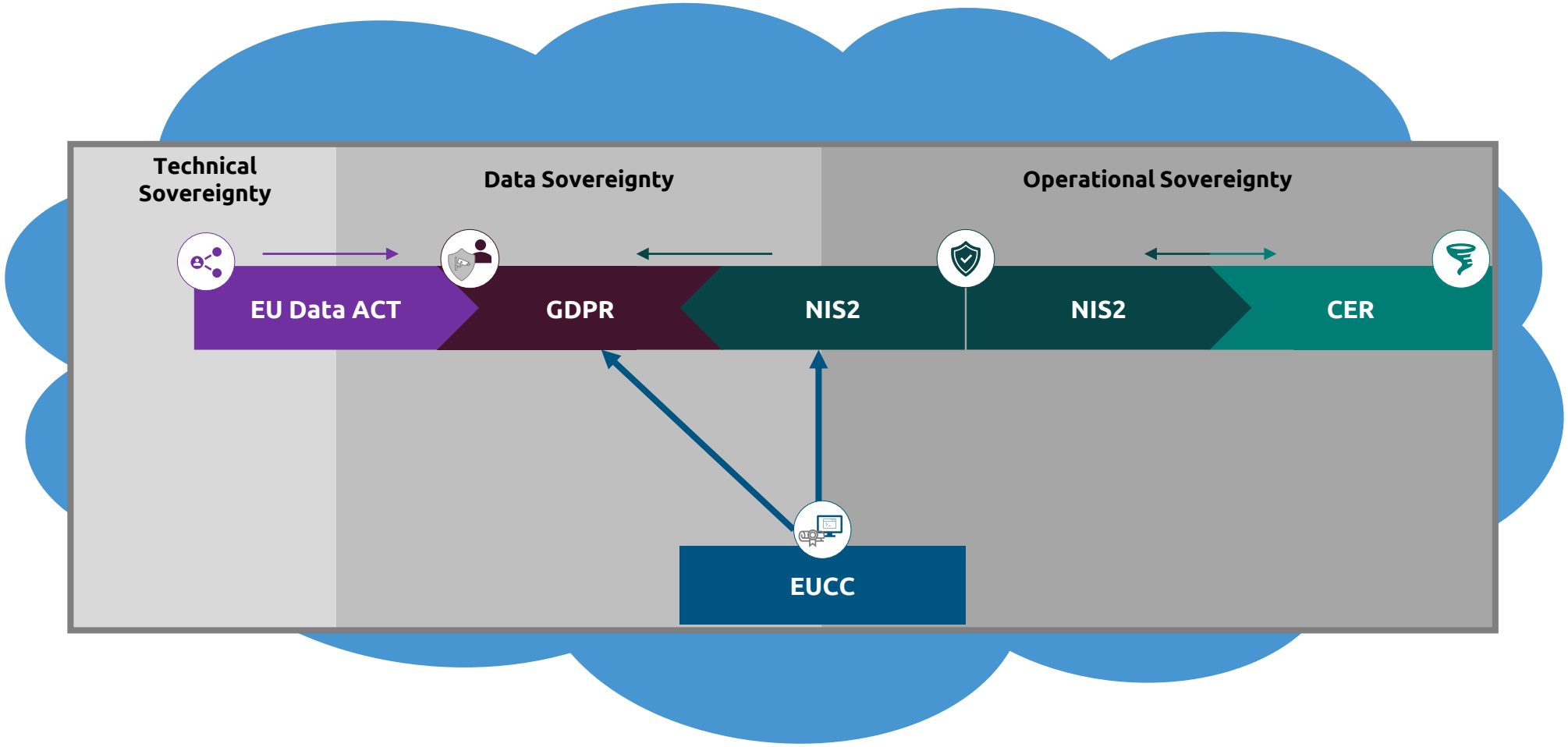
Active/enforced legislation

Most relevant directives and regulations in terms of cloud sovereignty

	EU Data Act	GDPR	NIS2	CER	EUCC (EUCSA)	EUCS (EUCSA)	BIO
Key element	To strengthen the EU's data economy and promote a competitive data market, the act ensures that data is fairly distributed, accessible and usable by different actors in the data economy. This will foster data-driven innovation and improve data availability	The GDPR is a comprehensive **data protection** and **privacy** regulation	NIS2 strengthens cyber security threat obligations for critical and important entities	The CER provides a comprehensive framework for improving the resilience of critical entities against physical threats	The EUCC scheme is a framework for evaluating and certifying the security features and capabilities of IT products and systems. It provides a set of internationally recognized standards and guidelines for assessing the security	The EUCS is a framework that applies only to cloud computing services. The EUCS aims to improve and streamline the cybersecurity of cloud services across the EU, categorizing them into four levels of assurance	The BIO defines concrete controls for information security for Dutch Governmental entities based on the NEN-ISO/IEC 27001 and NEN-ISO/IEC 27002
Contribution to cloud sovereignty	The Data Act will allow cloud users to easily switch CSPs, enable functional equivalence, gives users more control and choice over their data, and minimizes foreign access to European data	It protects sensitive and personal information by ensuring that cloud services meet strict standards concerning data processing, transfer, and protection. Cloud providers are held responsible for handling data with integrity and confidentiality	It contributes to cloud sovereignty by strengthening the resilience of cloud providers against cloud cybersecurity threats and by e.g. strengthening incident response for cloud services	This directive reinforces cloud sovereignty by strengthening the resilience of cloud providers' critical physical infrastructure, ensuring that cloud services can continue to operate	The EUCC scheme ensures cloud sovereignty by certifying that cloud infrastructure and services meet rigorous standards, increasing the security and resilience of their network and information systems and enhancing data protection	The EUCS strengthens cloud sovereignty by setting common (security) standards for EU-based cloud providers, ensuring clarity for users on EU rules and fostering trust in secure cloud solutions hosted in the EU	The BIO defines risk based security levels with concrete measures and controls per level of security and
Data sovereignty	X	X	X		X		
Operational sovereignty			X	X	X	X	X
Technical sovereignty	X					X	X

*plotting for BIO2.0 to be added

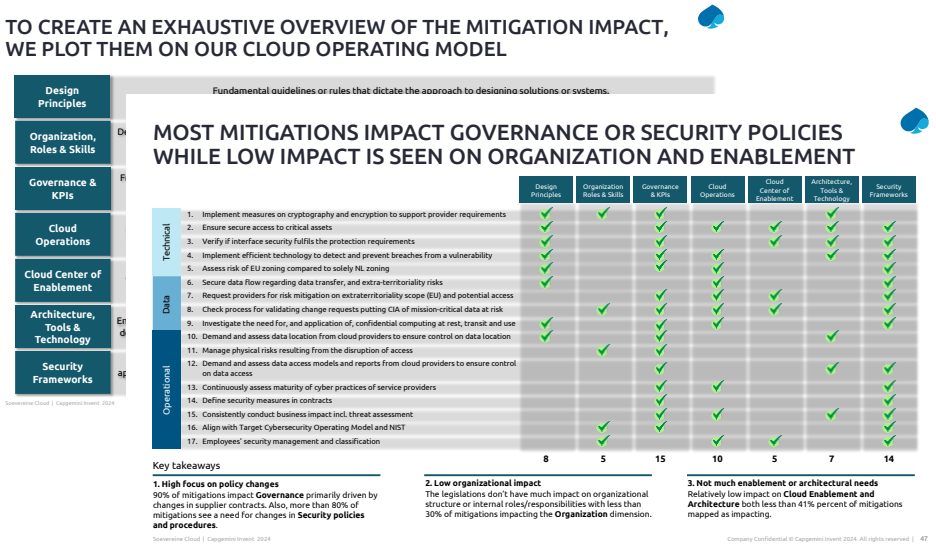
How do these legislations relate to the dimension of Sovereign Cloud



*plotting for BIO2.0 to be added

Our best practice to work towards compliancy

- Define the gap with the legislation
- Define mitigations to close the gap
- Use a framework to plot the compliancy



Developments and applications of sovereign cloud

Stefan Zosel
VP Sovereign Cloud Transformation
Global Public Sector

Linkedin

Capgemini

Sovereignty from the street:

01

We fear, that US Cloud Act access out data

But: Cloud Act is about telemetry data, not database content

02

It is a European specific challange

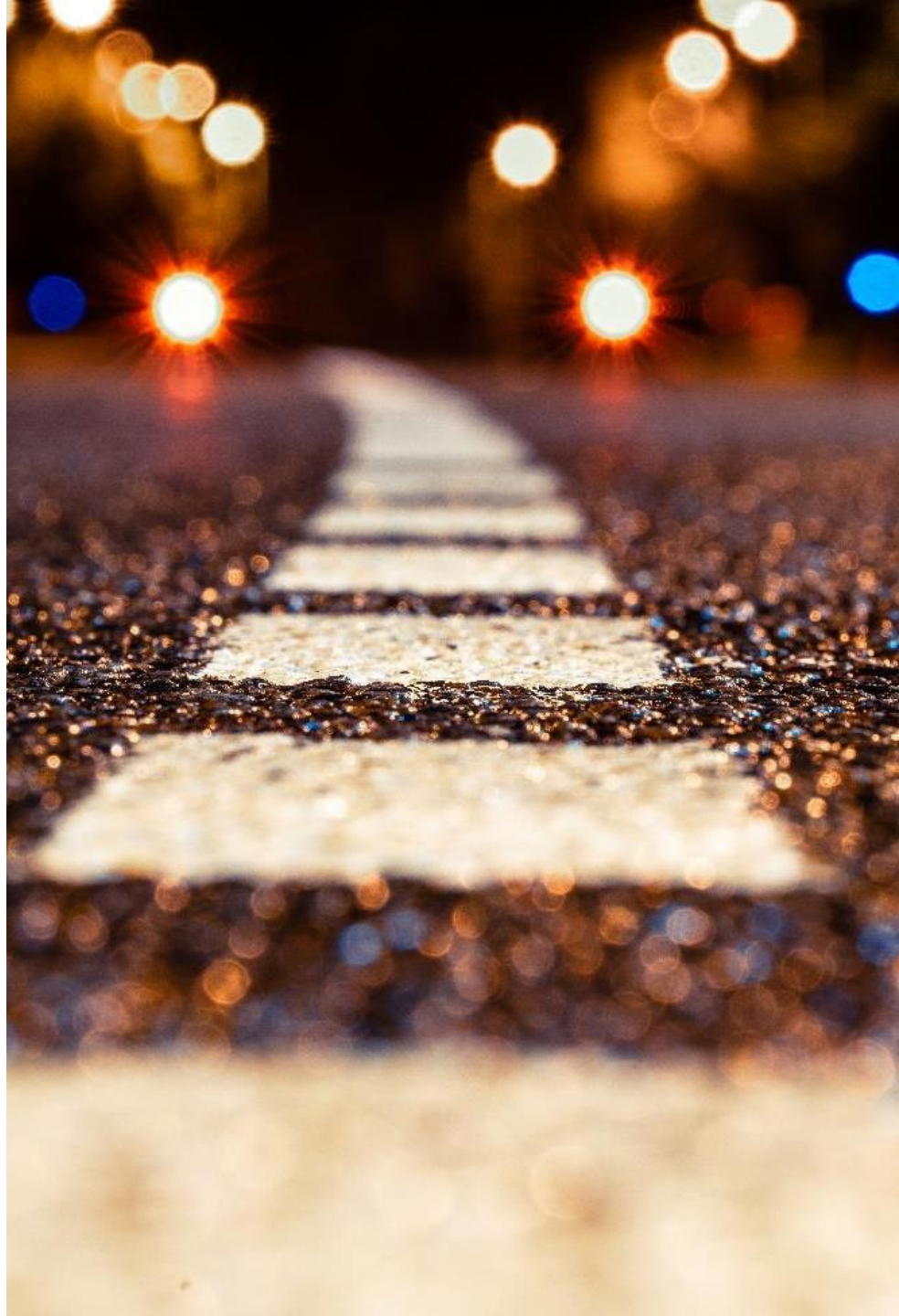
But: Major concerns & investments in Middle East, ignapore, Australia, …

03

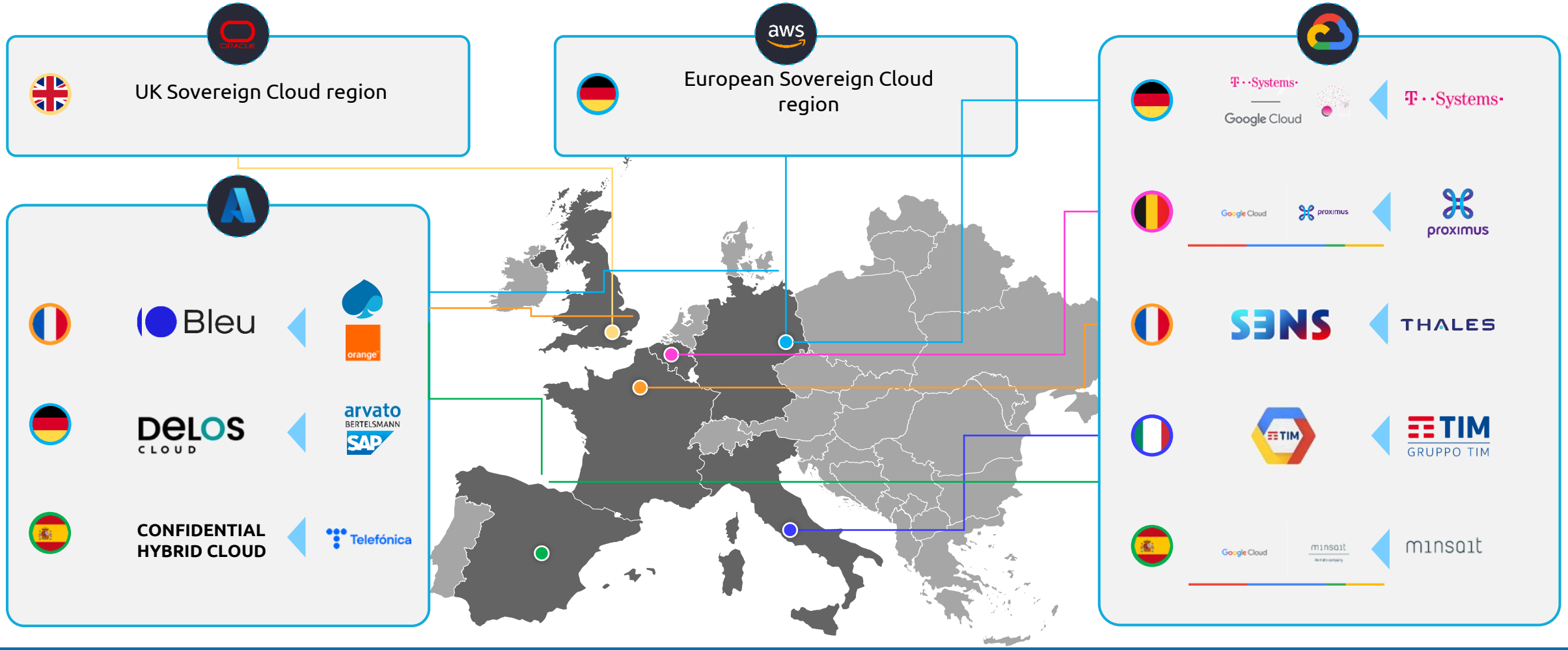
We fear, that US could disconnect EU from technology

But: AWS: Nitro is developed/operated from Germany
Azure: Managed Data out of Serbia
Azure: Denmark: Quantum Computing Research
Google: Poland biggest Development Center outside US and many more…

Where is the real thread?



There are a wide range of European sovereign cloud initiatives to leverage insight from



And also many local Cloud Providers

Lets zoom into Netherlands?

CSP understood the challange
and now more local/compliant offers are available

But: We should not forget EU perspective!
Learn from US: they are not limited to state level!

Zoom out on EU level to get best options!

Sovereign platforms in EU – Capgemini internal reseach

	BLEU	Microsoft	OVHCLOUD	IONOS	GOOGLE	ORACLE	AWS
UNDERLYING CLOUD TECHNOLOGY	Microsoft Azure	Microsoft Azure	OVHcloud (IaaS) Vmware (PaaS)	OSS Stack	German Sovereign GCP		
SOVEREIGN OFFER QUALIFIED (OR IN PROGRESS)	Azure Modern Work	Microsoft Cloud for Sovereignty	Hosted Private Cloud	Hosted Public/ Private Cloud	GCP Sovereign Cloud	OCI Oracle Sovereign Cloud	AWS Sovereign Pledge
OFFERING	SAAS	M365 In 2 ~ 4 yrs	No SAAS	No SAAS	SAAS	SAAS – ORACLE LEGACY	SAAS
	PAAS	PAAS	PAAS	PAAS	PAAS	PAAS	PAAS
	IAAS	IAAS	IAAS	IAAS	IAAS	IAAS	IAAS
COLLABORATION	YES – M365	M365 In 2 ~ 4 yrs	NO	OSS Based Sovereign Desktop	Google Suite – but not EU Sovereign/resident!	NO	NO
MARKETPLACE	YES	YES	YES	YES	YES	YES	YES
OWNERSHIP	Capgemini 50% Orange 50%	US	Family Owned	Family Owned, Public Traded	T-Systems Google	US HQ SOV Cloud OCI Germany Entity	AWS/US
AVAILABILITY	2025	Available	Disponibles SNC3.1	Available	Available	Available	AWS EU Sov Cloud Exp. 2025

STATUS END OF 2023

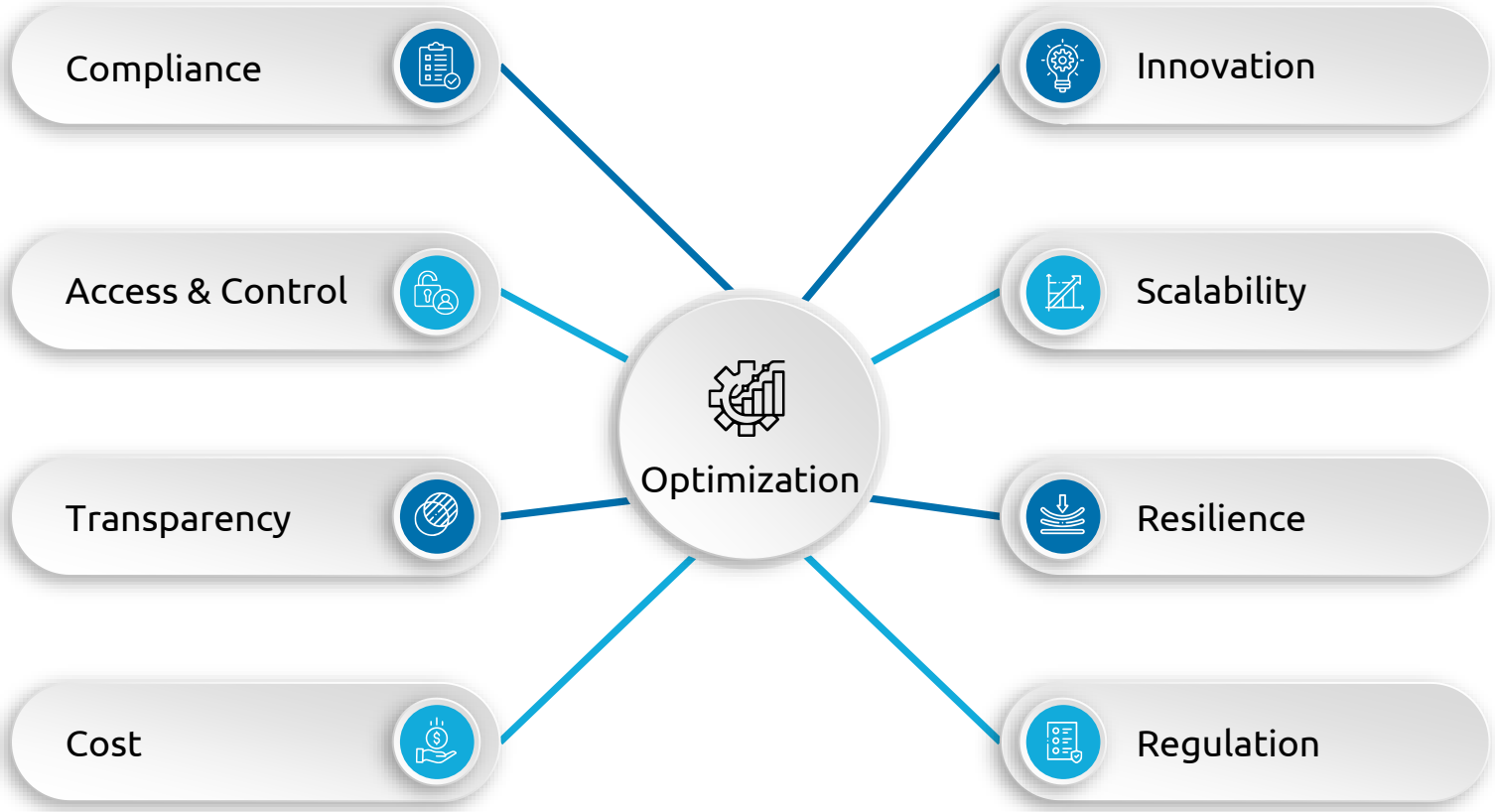
Sovereign cloud deployment models

The cloud migration journey can follow multiple paths, and **new sovereign** and **trusted cloud solutions** come further **broaden the picture**.

	PRIVATE CLOUD	COMMUNITY CLOUD	HYBRID CLOUD	PUBLIC CLOUD		
				Hyperscaler Sovereign Cloud	Open Sovereign Cloud	Restricted Sovereign Cloud
Description	• Infrastructure sits within a **private network dedicated to the owner's use only** • Infrastructure can be hosted **externally** or on **the premises** of the owner	• Several (but a limited set of) companies **share private infrastructure**, usually owned by **one of the users or a 3rd party**	• Combine the **best of two worlds (public & private)** to create a unique cloud setup tailored to business & IT needs or constraints	• Infrastructure belongs **3rd party**, the public CSP, who **administers the pool** resources • Infrastructure **shared with the other clients** of the CSP	• Cloud computing environment **deployed, operated, secured and maintained locally within a single national jurisdiction**	• A sovereign cloud provider which obtained the "trusted cloud" label through a **national certification delivered by local governmental** organization
Main features	• **Better control** over data, users & information assets • **Enhanced security** with customizable features to meet the client's needs • **Improved performance** (with customizable SLAs) • **High customization** level of the hardware & software resources	• **Balanced tradeoff** between public and private deployments • Shared infrastructure between companies with **similar security**, privacy, **performance** or **compliance** requirements • **Lesser savings than costs spread over fewer users** than the public cloud	• **Customizable tradeoff** between public cloud capabilities and private cloud security • High **flexibility in architectural and security decisions** • **Scalable and cost effective** • **Business continuity** and **disaster recovery** also enabled	• Broad range of services and **innovative offerings** (AI/ML, VR, etc.) • **Constantly evolving** and improving service catalogs • Large **economies of scale** achievable at high volumes • **Pay-as-you-go** model (no upfront charges or bandwidth fees) • **Key Management** HSM/BYOK *+ Other national & EU providers are also included on this section.*	• **GDPR** compliant • **Customer's data** are located in Europe • **Technical support** requests & **access** will be fulfilled by an **EU-authorized person** located in the EU • Custom **encryption and partitioning** system for **sensitive data** • Easy deployment of controls for **workloads** with **security requirements** (residency, access management, etc.)	• Improved **immunity from extraterritorial laws** • **Stricter access** from non-EU individuals • **All data** located in Europe (ex. technical data) • Additional **security features** (limited data transfer) • **Better monitoring solution and audits** to prevent any incident • **Optimal business resiliency** & disaster recovery
	cisco, IBM, DELL, openstack.	salesforce, Azure	Azure Arc, AWS EKS Anywhere, Anthos	aws, Google Cloud	OVH.com, IONOS CLOUD	BLEU, DELOS CLOUD
	Secured cloud services				**Data sovereignty**	**Legal immunity**

No One-Size fits all – ist a diverse world!

Sovereignty is to optimize for:

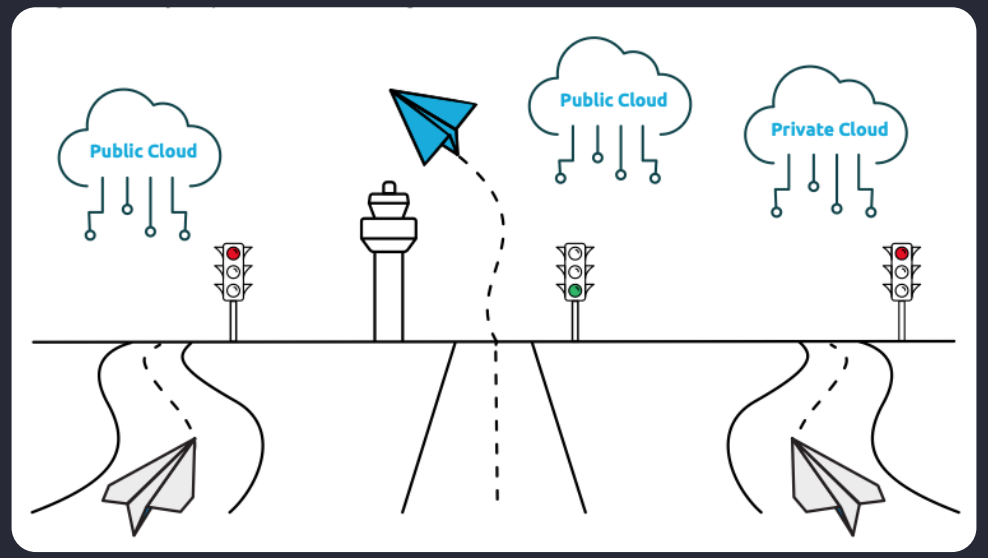


Which is the right platform for my use - case?

Making it real – point of view

Free to download

Four steps to implementing sovereign cloud identifies a safe way to benefit from the public cloud



QR Code – Making it real

There are alternative Operating models to assess sovereign cloud…

Geographic Options

- **Localization** of sovereignty: Sovereign EU region vs **country specific** regions with fully localized sovereignty.
- **Resilience**: two distinct regions each with two + availability zones vs single region with two availability zones, vs **single availability zone**.

Sovereignty Levels

What is Sovereign? The **entire shared responsibility model** vs only the consumer side.

- Infrastructure **Sharing**: Single vs Shared Tenancy of all infrastructure, networking and control planes (**depends on partner**).
- **Operational** Sovereignty: whether to offer software / service provider independence to guarantee portability for fixed periods vs a more **"locked-in"** approach.
- **Assurance** levels: which assurance and certification standards to offer out-the-box compliance with, e.g. commercial, **restricted**, secret; **ISO27001**, SP800-r53, NATO- Restricted).

Realisation Approach

- Value added services, **accelerators and resources** (etc.) building above a CSP's existing public cloud.
- Partner with a CSP to resell their cloud-on-prem or **public region** offers hosted from Telenor datacenters.
- IaaS Only – creating a new offer to compete with the CSPs on an IaaS basis..
- Datacenter space as a service with the offer limited to space, power, cooling and network connectivity.

Organisational Model

Shared **Responsibility** Model, describing how consumers and partners share responsibility and interact.

Option 1 and think about shared responsibility model

		SaaS	PaaS	IaaS	onPrem
Responsibility always retained by the customer	Information and Data	Customer	Customer	Customer	Customer
	Devices (Mobile/PC)	Customer	Customer	Customer	Customer
	Accounts and identities	Customer	Customer	Customer	Customer
Responsibility varies by type	Identity and Directory	Shared	Shared	Customer	Customer
	Applications	CSP	Shared	Customer	Customer
	Network Controls	CSP	Shared	Customer	Customer
	Operating Systems	CSP	CSP	CSP	Customer
Responsibility transfers to cloud provider	Physical Hosts	CSP	CSP	CSP	Customer
	Physical Network	CSP	CSP	CSP	Customer
	Physical Datacenter	CSP	CSP	CSP	Customer

Customer | Shared | CSP

and extend it to „sovereign controls“

		SaaS	PaaS	IaaS	onPrem
Responsibility always retained by the customer	Information and Data	Customer	Customer	Customer	Customer
	Devices (Mobile/PC)	Customer	Customer	Customer	Customer
	Accounts and identities	Customer	Customer	Customer	Customer
	Identity and Directory	Customer	Customer	Customer	Customer
	Applications and Resilience	Customer	Customer	Customer	Customer
	Compliance Controls	Customer	Customer	Customer	Customer
	Encryption / Conf. Compute	Customer	Customer	Customer	Customer
Responsibility varies by type	Network Controls	CSP	Shared	Customer	Customer
	Operating Systems	CSP	CSP	CSP	Customer
Responsibility transfers to cloud provider	Physical Hosts	CSP	CSP	CSP	Customer
	Physical Network	CSP	CSP	CSP	Customer
	Physical Datacenter	CSP	CSP	CSP	Customer

Sovereign on cloud with full control and compliance

Cloud scalability and functions

Customer | Shared | CSP

Example from Nordics – Healthcare / Patient Data

Case & transaction management

Personalize engagement

Automate customer service

Streamline operations

PEGA

Encryption

+Speed

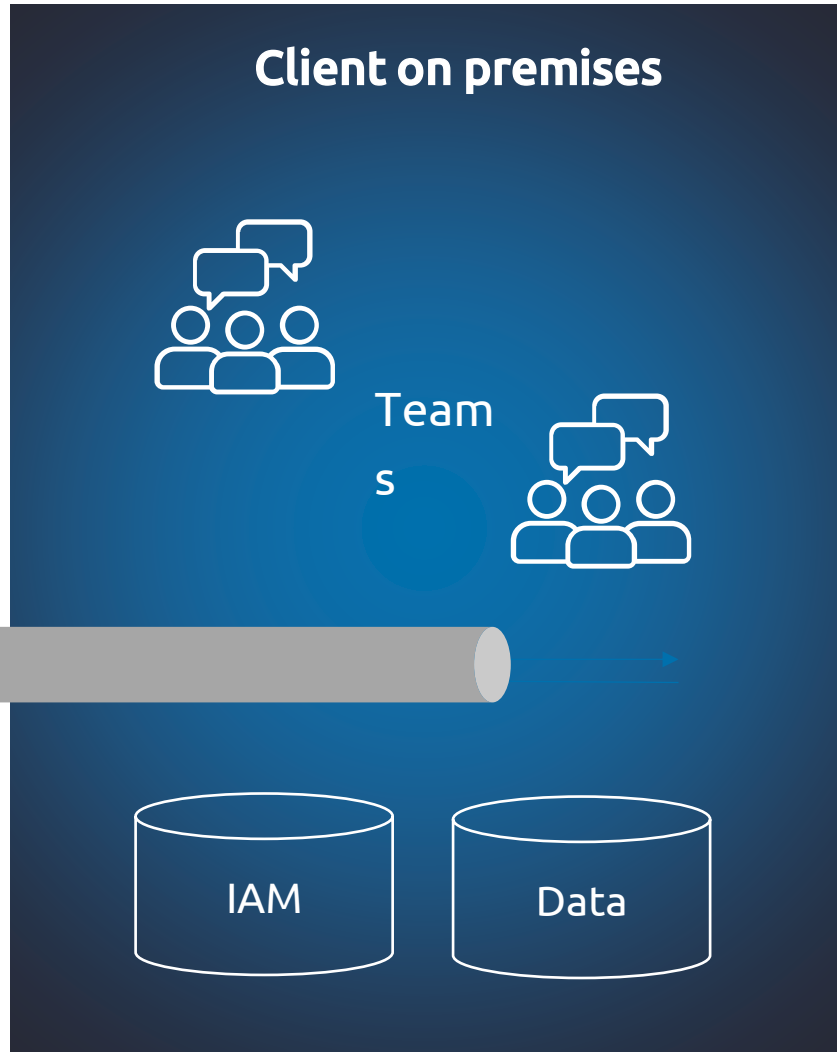
+Cost Savings

+Patient experience

aws

Region:

Sweden/Stockholm



DEV RUN

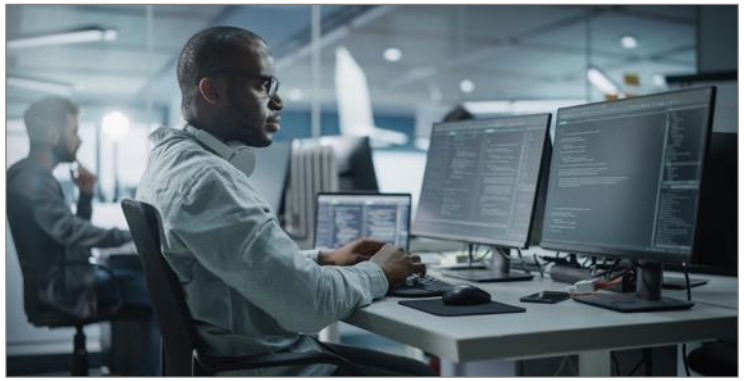
Secure software factory

Dev Low/Run High to digitize restricted business processes

Enabling our clients to benefit from the velocity and economics of modern cloud

Capgemini

Example: Agile development in defense



- Development and Operations is clearly separated and air-gapped.
- Environment is highly regulated and secure.
- How to innovate and optimize modern IT?

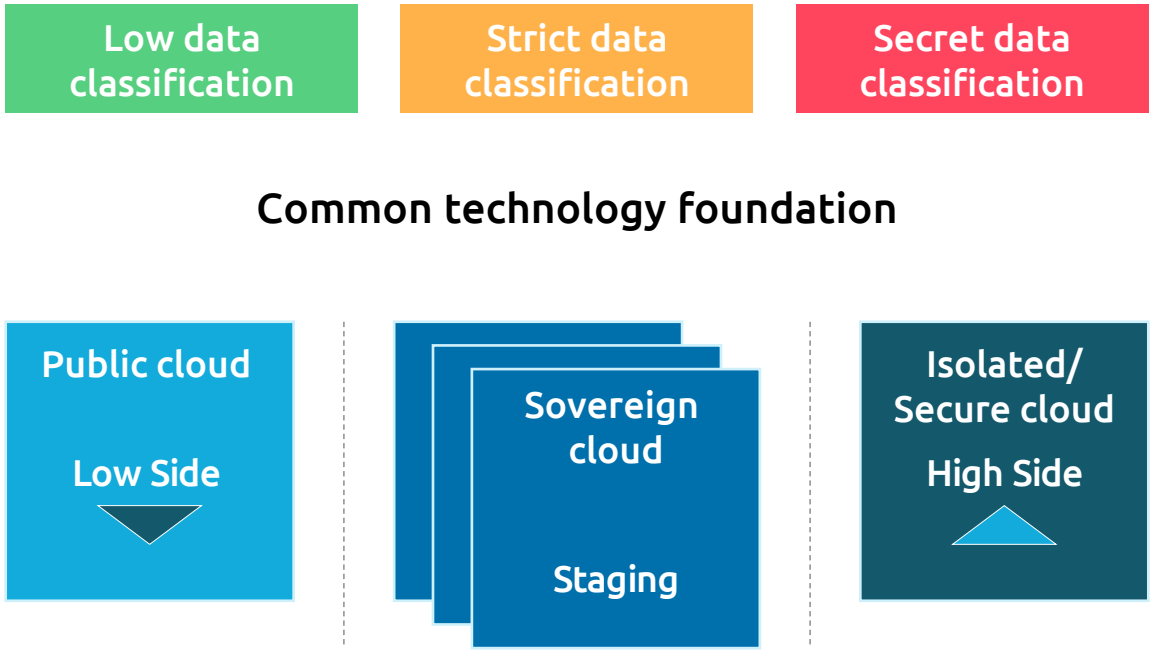
Sensitive → Secret → Top secret

Capgemini defense use-case

Secure Cloud Software Factory

Development on low side:

- Access to innovation
- Easy to staff
- Best practices
- Reduce cost

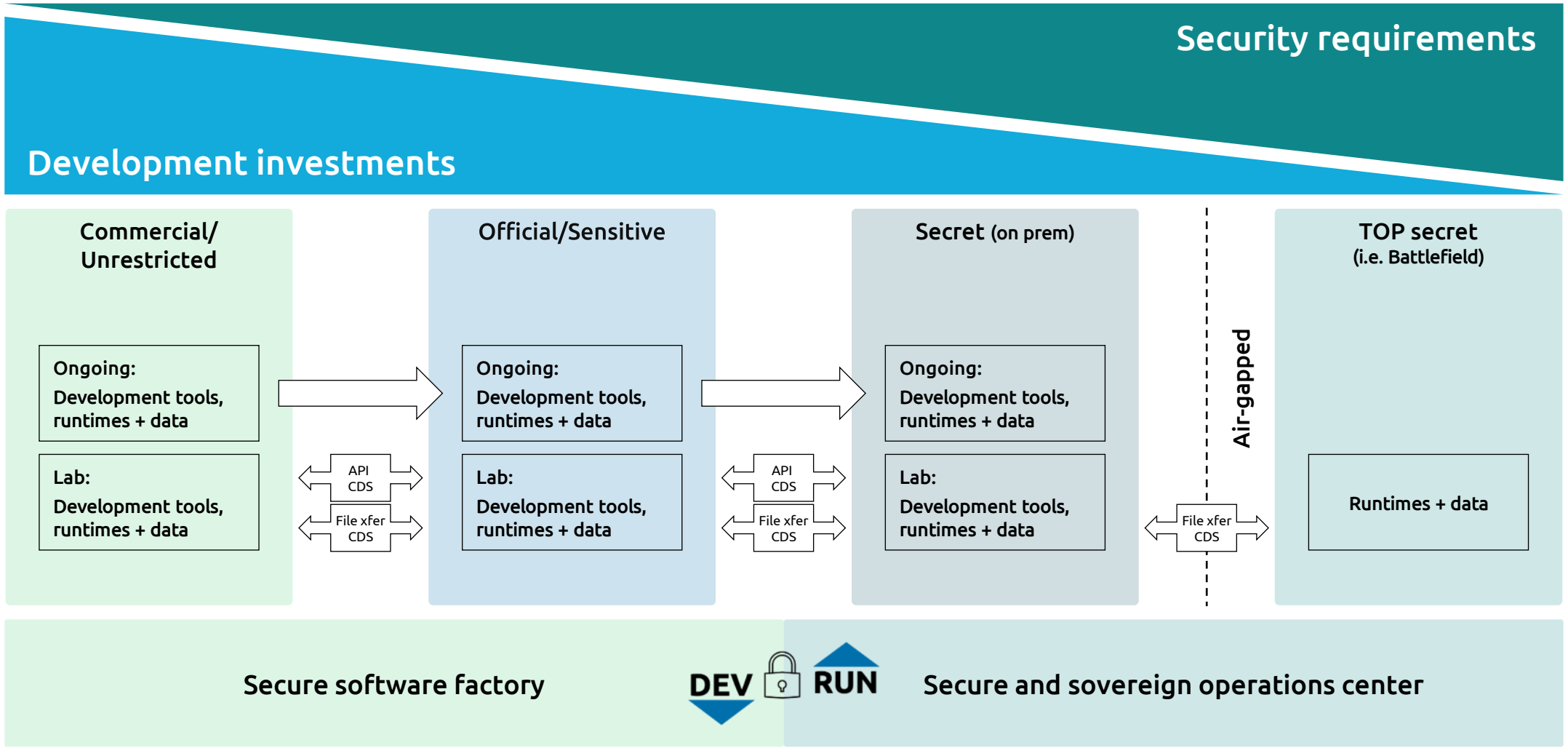


Run on high side:

- Secure operations
- Compliance
- High security
- Limited access
- Control
- Less classified staff

De-couple development from security Operations

It’s not just low and high



Thank you

Stefan Zosel
Global Public Sector Cloud Lead

stefan.zosel@capgemini.com

Get the future *you* want

Capgemini

capgemini.com

Vision Cloud Service Providers on Sovereign Cloud

Michiel van Otegem

Cloud Sovereignty Architect / Global Engineering, Microsoft

Julien Blanchez

Digital Sovereignty Solution Lead, Google

Alex Meek Holmes

Global Business Development - Sovereignty and Infrastructure, AWS

Capgemini