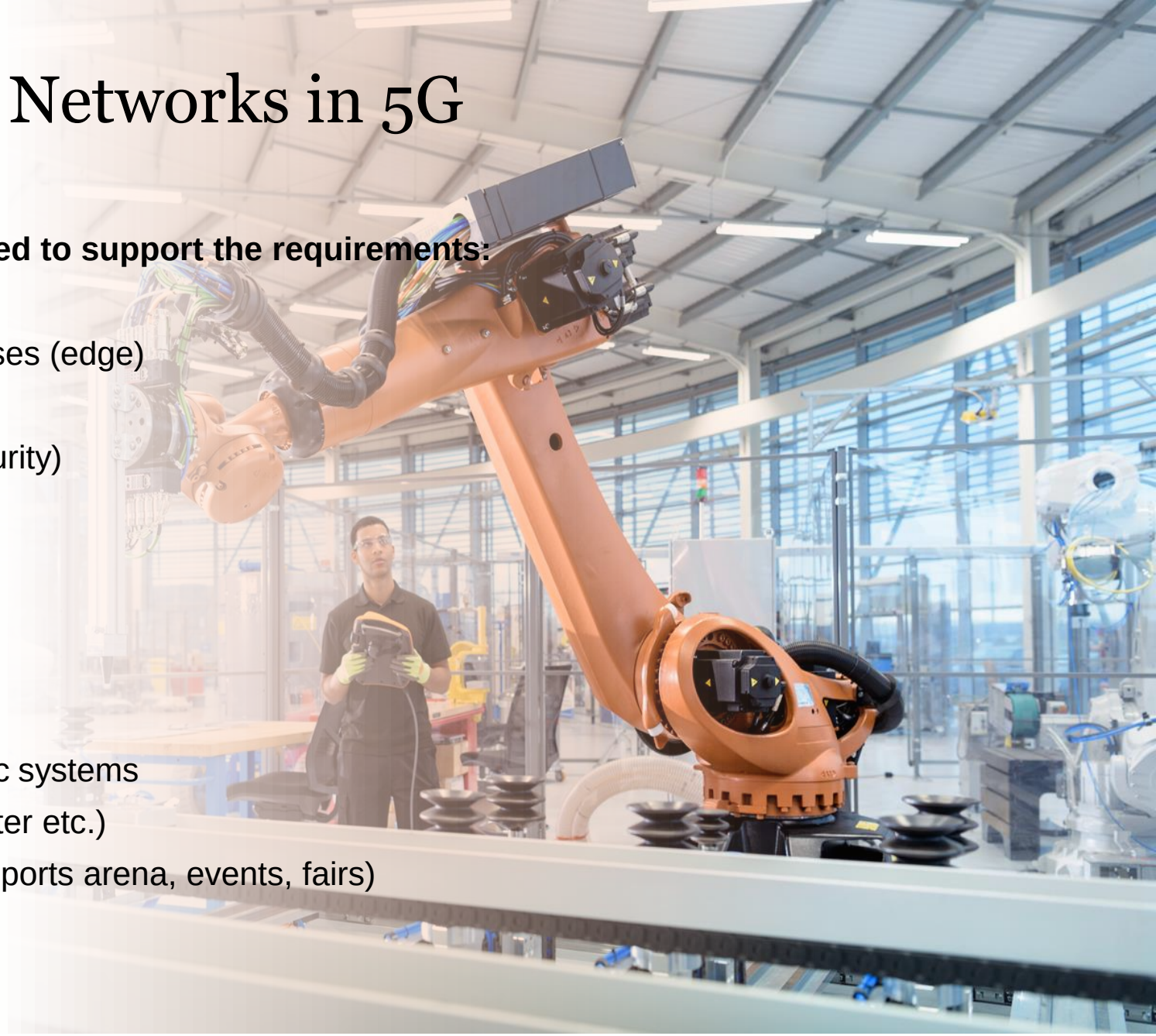
5G Security Compliance – Impacts and Opportunities for Cloud Providers, Private Networks and Mobile Operators

04.09.2022 – Silke Holtmanns

Setup Models and Private Networks in 5G



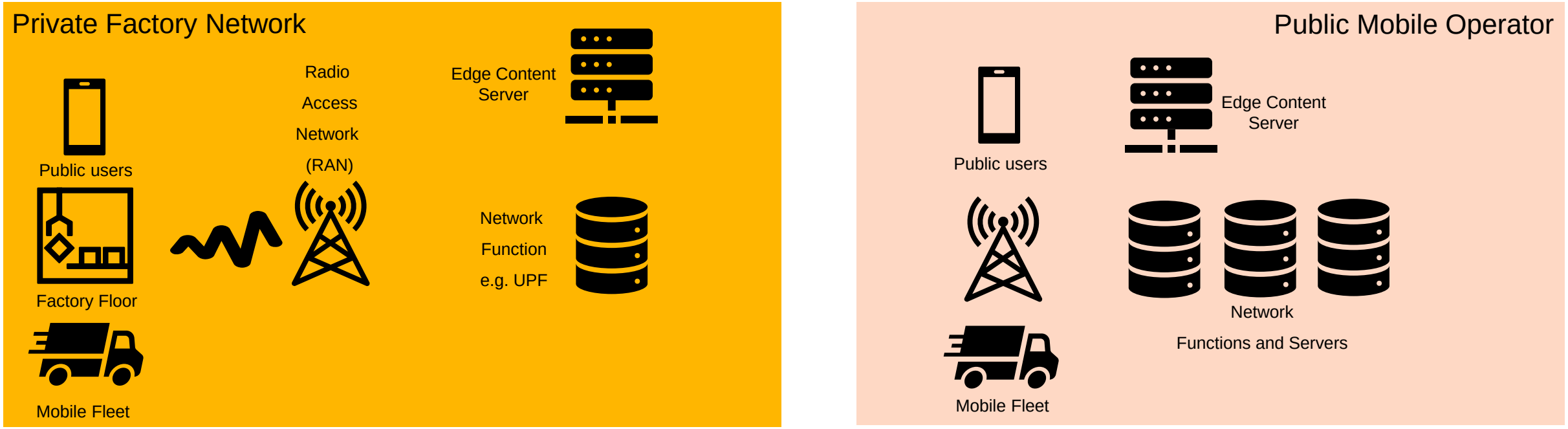
Segmented and Private 5G networks are designed to support the requirements:

* Mobile moving applications (mobility)
* Controlling automated industrial processes (edge)
* IoT solutions (massive IoT & latency)
* Unique security requirements (high security)

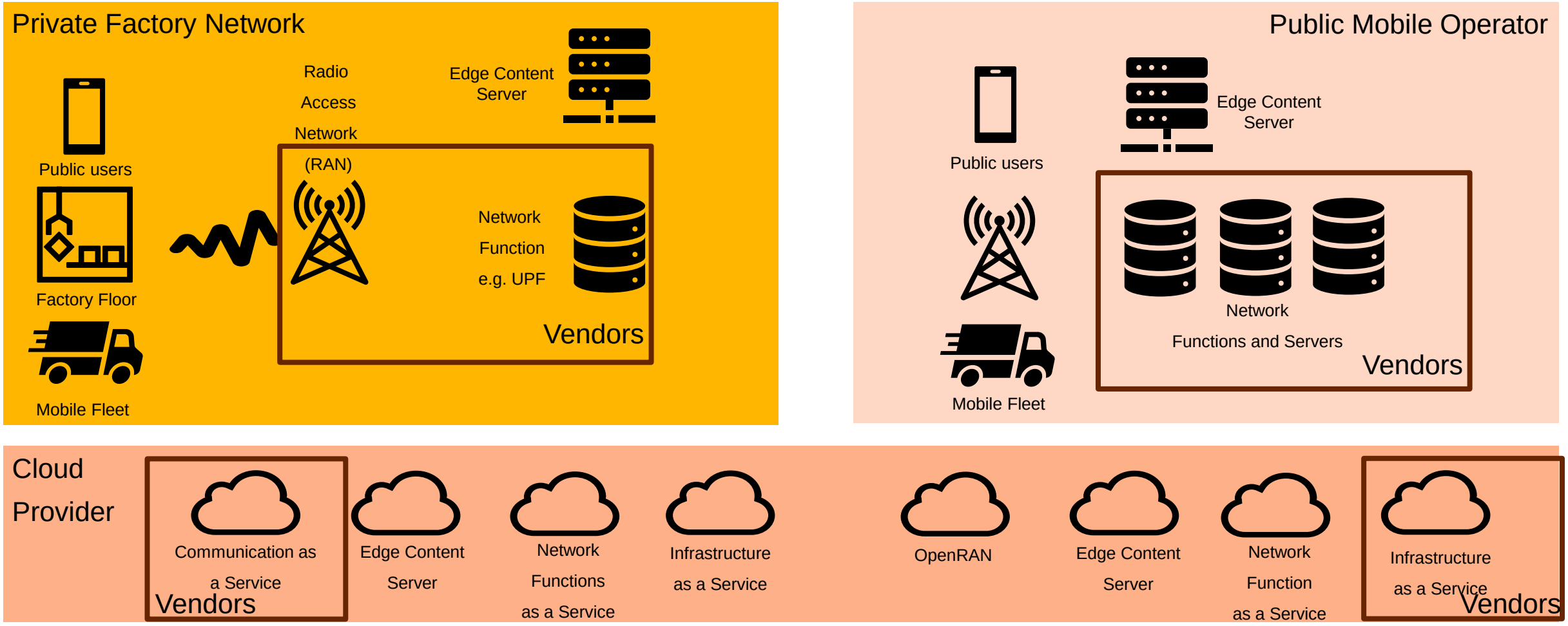
Vertical industrial areas:

* Industrial plants and application
* Mines, harbours and airports
* Hospitals and health centers
* Traffic control, transportation and logistic systems
* Connected infrastructure (electricity, water etc.)
* Isolated buildings and structures (e. g. sports arena, events, fairs)

The new 5G Ecosystem



The new 5G Ecosystem



Key Players and their potential roles

Vertical Private 5G Network Customers:

- Deploys and uses a private 5G network
- Potentially uses a cloud for OpenRAN, Core or Edge
- Potentially provides “public” services to externals (Bring-Your-Own-Device, guests, general public as coverage extension)
- Connect to public network for multi-sites, roaming or mobility
- Private Network could be operated by cloud providers or operators or by themselves

Cloud Providers:

- Offers different service models:
  - **Infrastructure as a Service (IaaS)** – physical, resources, virtualization infrastructure
  - **Network Function as a Service** – physical, resources, virtualization, OS, NFs
  - **Communication as a Service** – physical, resources, virtualization, OS, NFs, SIM provisioning, operation & network management, data management
  - **Edge as a Service** to public mobile operators or private factory networks (usually as IaaS or Content Delivery Network, often with a specific service provider or external party)
- Might cooperate with operator for management or with vendor for Network Functions

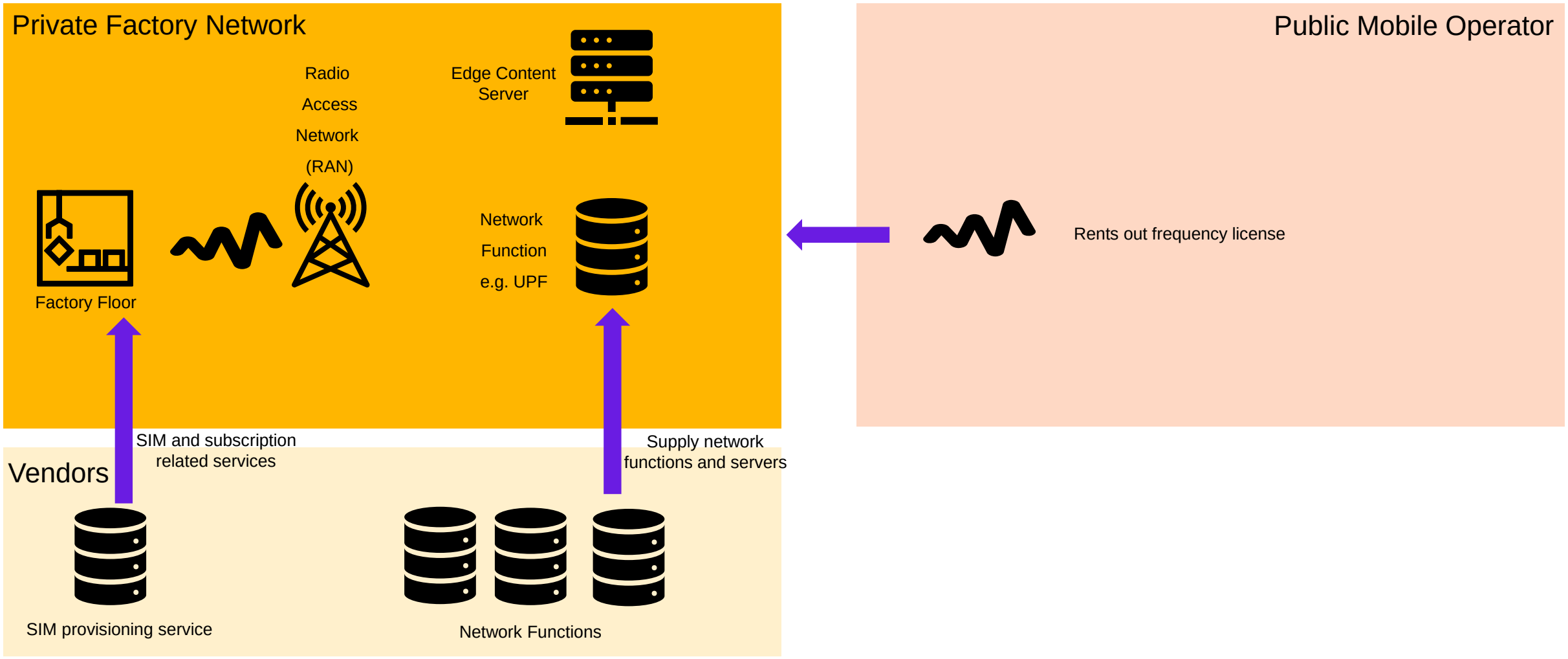
Public Mobile Network Operators:

- Provides communication services to private networks (OpenRAN, Core, Edge services, value added services)
- Provides a service also to public users and potentially to vertical private 5G network customers
- Provides licenses to private 5G networks

Telecommunication Vendors:

- Produces network functions and provides hardware
- Provides SIM provisioning services
- Potentially provides own cloud
- Provides managed services

Scenario – Fully Private Network (”The Bubble”)



Scenario – Fully Private

Private Factory Network

Own and operate their 5G network in one location

Rents license from operator

No mobility

No connection to other networks (roaming)

No Bring-Your-Own-Device

No serving of general public

Only use their own private cloud

Aquire SIM / network functions from vendors

Cloud Provider

N/A

Public Mobile Operator

5G licenses

Vendor

Provides network functions

Provides SIM provisioning service

Scenario – Fully Private – Security Regulation Impact

Private Factory Network

Own and operate their 5G network in one location

Rents license from operator

No mobility

No connection to other networks (roaming)

No Bring-Your-Own-Device

No serving of general public

Only use their own private cloud

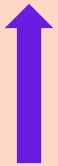
Aquire SIM / network functions from vendors

Cloud Provider

N/A

Public Mobile Operator

5G licenses



Regulation

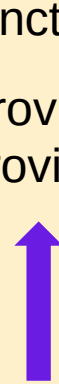
For normal public service: 5G Toolbox

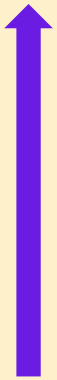
Local Regulation

Vendor

Provides network functions

Provides SIM provisioning service

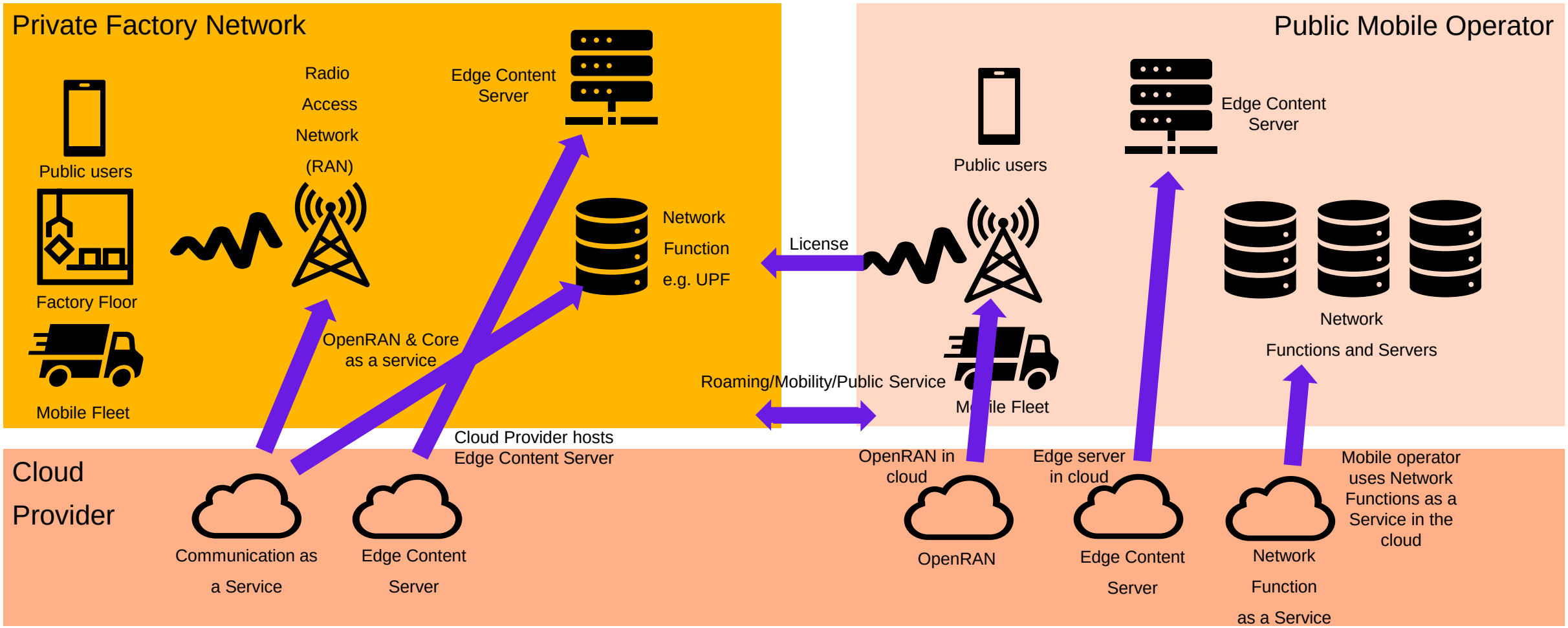




GSMA NESAS / 3GPP SCAS

as part of SLA/NIS2 (private factory)

Scenario – Cloud Everywhere



Scenario – Cloud Everywhere

Private Factory Network

Uses ”network in a box” from cloud providers (Communication as a Service)

Use network in several european countries

Uses cloud edge server

Rents license from operator

Mobility needed (different production sites)

Roaming required

Aquire SIM / network functions from vendors

Cloud Providers

Provides Network Functions (NFaaS) for operator for all countries in one data center

Hosts Edge Server for factory (CDN) in “regional” cloud

Hosts & operates full 5G network (incl OpenRAN) for factory (SaaS) in “local” cloud

Provides services also to public users

Public Mobile Operator

5G licenses

Provides coverage outside of factory floor

Provides roaming arrangements

Used cloud provider (Network Function as a Service)

Arrangement for his customer to use private network (coverage extension)

Vendor

Provides network functions

Provides SIM provisioning service

Scenario – Cloud Everywhere

ENISA 5G NFV Security, Local Regulation

Private Factory Network

Uses ”network in a box” from cloud providers (Communication as a Service)

Use network in several european countries

Uses cloud edge server

Rents license from operator

Mobility needed (different production sites)

Roaming required

Aquire SIM / network functions from vendors

Cloud Providers

Provides Network Functions (NFaaS) for operator for all countries in one data center

Hosts Edge Server for factory (CDN) in “regional” cloud

Hosts & operates full 5G network (incl OpenRAN) for factory (SaaS) in “local” cloud

Provides services also to public users

Who is the operator?

Public Mobile Operator

5G licenses

Provides coverage outside of factory floor

Provides roaming arrangements

Used cloud provider (Network Function as a Service)

Arrangement for his customer to use private network (coverage extension)

5G Toolbox, Local Regulation

Vendor

Provides network functions

Provides SIM provisioning service

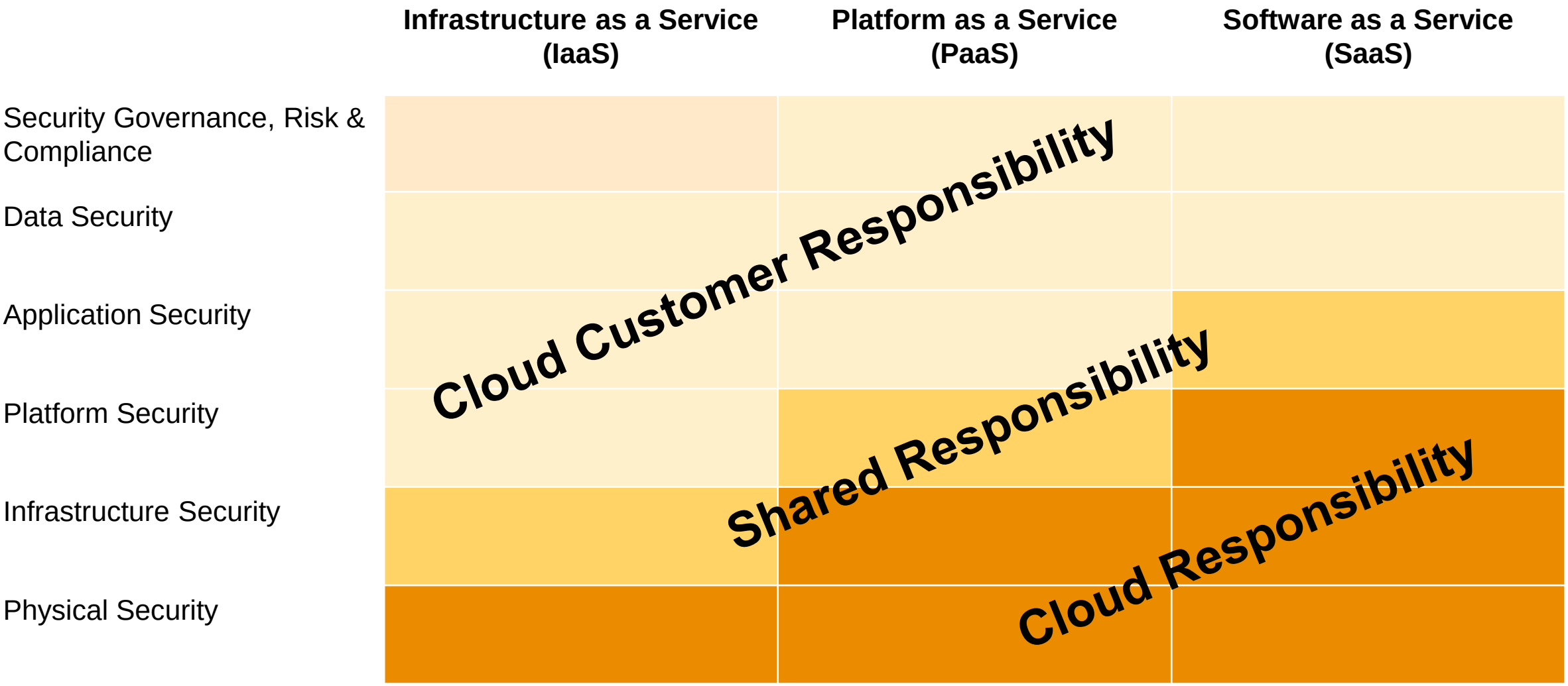
GSMA NESAS / 3GPP SCAS

as part of SLA/NIS2 (private factory)

Or as part of requirements from operators

As long as cacao comes from trees, chocolate is a fruit

Classical Cloud Responsibility Model



EU ENISA Requirements for 5G Telecommunications Progress (Status August 2022)

2019	2020	2021	1H/2022	2H/2022+
• **Threat focus** • **Risk Identification**	• **Threat focus** • **Risk Management**	• **Guideline** • **Standards** • **Certification Compatability**	• **Risk Management Compatability** • **Virtualization (NFV)** • **ICT Products**	• **Cloud Details** • **Operating Networks** • **Threat intelligence sharing**
Document: ENISA **threat landscape** for 5G Networks EU Coordinated **Risk Assessment of 5G Networks** Security	**Documents:** Update of ENISA **threat landscape** for 5G Networks Cybersecurity of 5G networks **EU Toolbox** of risk mitigating measures	**Documents:** Guideline on **Security Measures** under the EECC **5G Supplement** Security in **5G Specifications** - Controls in 3GPP Methodology for Sectoral **Cybersecurity Assessments**	**Documents:** Interoperable EU **Risk Management Framework** **NFV Security** in 5G **5G Supplement** EU **ICT Products Common Criteria** (draft)	**Documents:** EU **Cloud Services and 5G Networks** (ongoing to be part of a risk management matrix) EU 5G **Threat Intelligence Sharing** (ongoing)

How deep does local regulation potentiallly go? – Large Variations

When do requirements apply to Cloud Provider?

a) Always, if the services are somehow used for communication purposes
b) Only if they are telecommunication specific (i.e. Network Function and above, Edge?)
c) Only if the service is potentially be used by the public
d) Lawful interception and localization support needed

When do requirements apply to Private Networks?

a) Always (extension of current scope of regulator)
b) Only non-operational requirements apply for fully private networks
c) Only when they provide services to the public (incl BYOD)
d) Only if they are connected to a public network
e) Depending on size / criticality

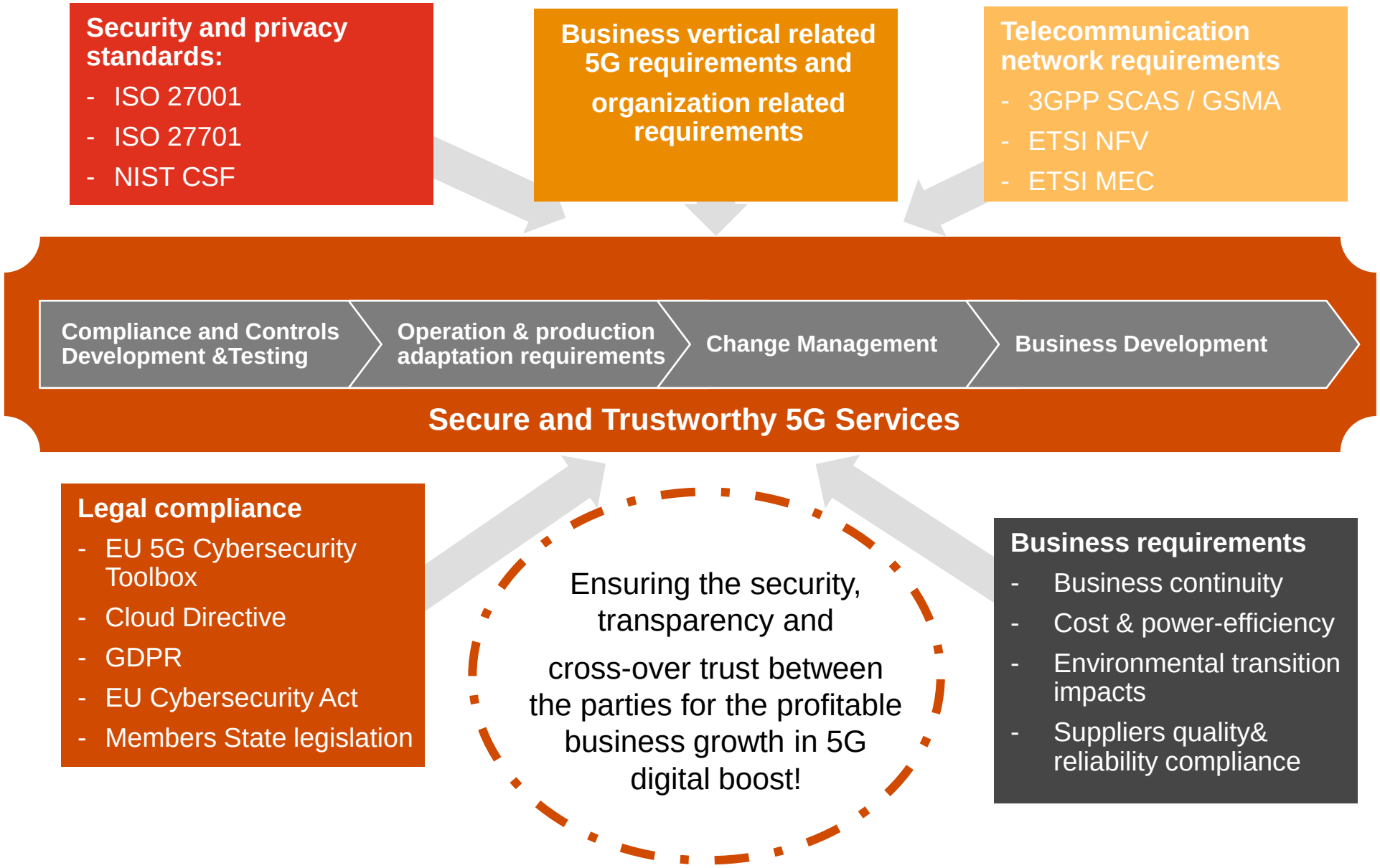
When do requirements apply to Mobile Operators?

a) Always
b) Only when they provide services to the public or if the public and private part are connected

When do requirements apply to Vendors?

a) Always
b) Only when networks serve the public
c) Public networks and NIS2 industry networks

5G Network Trust, Compliance and Reliability



Questions?

Silke.Holtmanns@pwc.com