Securing the “Sky”: Cloud Integrity and Audit

21.03.2025

Agenda

01 Who are we?

02 Types of Cloud

03 Cloud Integrity

04 Our Audit Approach

05 Q&A

1. Who are we?

With you today….

Jan Eberle

Director
Risk Assurance,
PwC

Carina Allmann

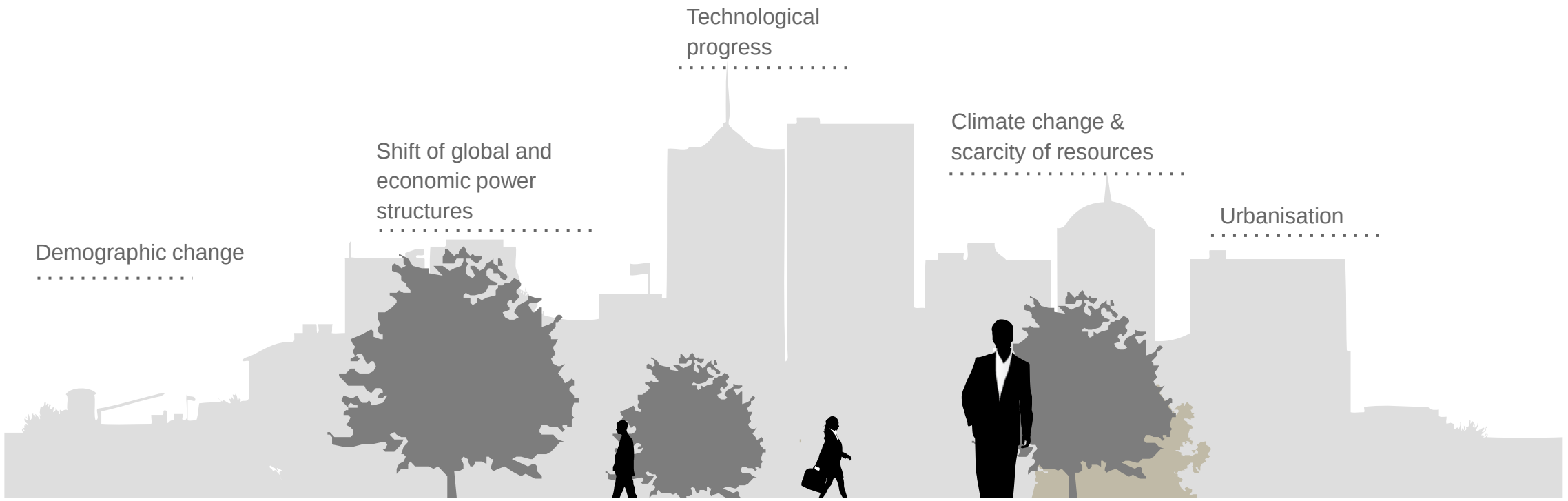
Manager
Risk Assurance,
PwC

Eduard Obernauer

Senior Associate
Risk Assurance,
PwC

Our purpose

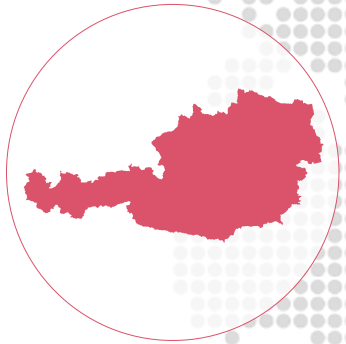
To build trust in society and solve important problems



Handling social challenges	Creating a sense of togetherness	Solving complex problems	Developing individual and trust-based relationships

PwC Austria and the international PwC network*

Austria
- More than 1,450 employees
- 5 locations
- Revenues: €212.6m



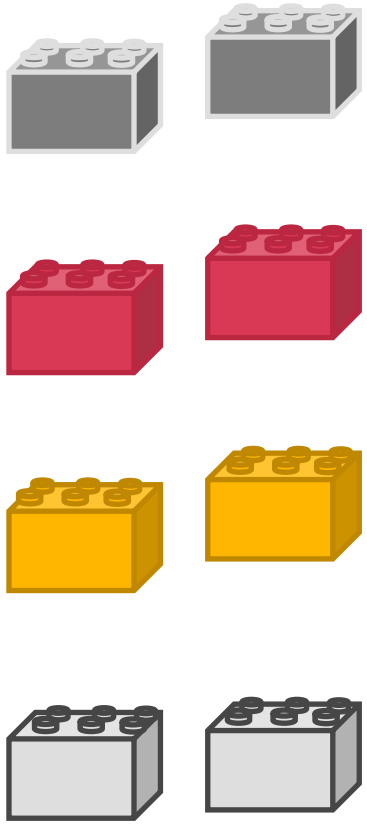
International
- More than 370,000 employees
- Locations in 149 countries
- Revenues: US$55.4bn

2. Types of Cloud

“The Cloud” is like saying “IT”. It's a concept, not one thing.

Building Blocks

It’s not a ‘black box’.... but built up of many blocks that you can mix and match - all this is **available in a few clicks** and easily integrated



Business Process as a Service (BPaaS)
Think... have someone else "do" stuff
Takeover of business processes
Ex: Payments, AR, eCommerce

Software as a Service (SaaS)
Think... how you “use/apply” Stuff
Business Applications to create value
Ex: Finance, ERP, CRM, etc. applications

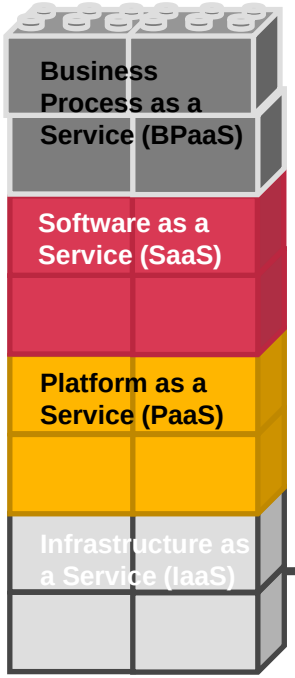
Platform as a Service (PaaS)
Think... how you “run” Stuff
Easier and faster tech to support your bus apps
Ex: Natural Language Processing, AI Models, WebApp deployment platform

Infrastructure as a Service (IaaS)
Think... where you “store” Stuff
Capacity, Data Storage, Network and Connectivity
Ex: Servers, “pipes/plumbing”

Finished Product

New Applications, bots, predictive maintenance, global deployments, etc. with a **Pay as you Go Model**

Combine and pay for **only the Blocks you need** - create a 10 room castle or a 2 room house



New, integrated applications

Predictive Analytics

Connected Supply Chains

Bots

Real-time Financial Close

and much more…

Predictability
Scalability
Agility
Accessibility

Example of clouds

IaaS

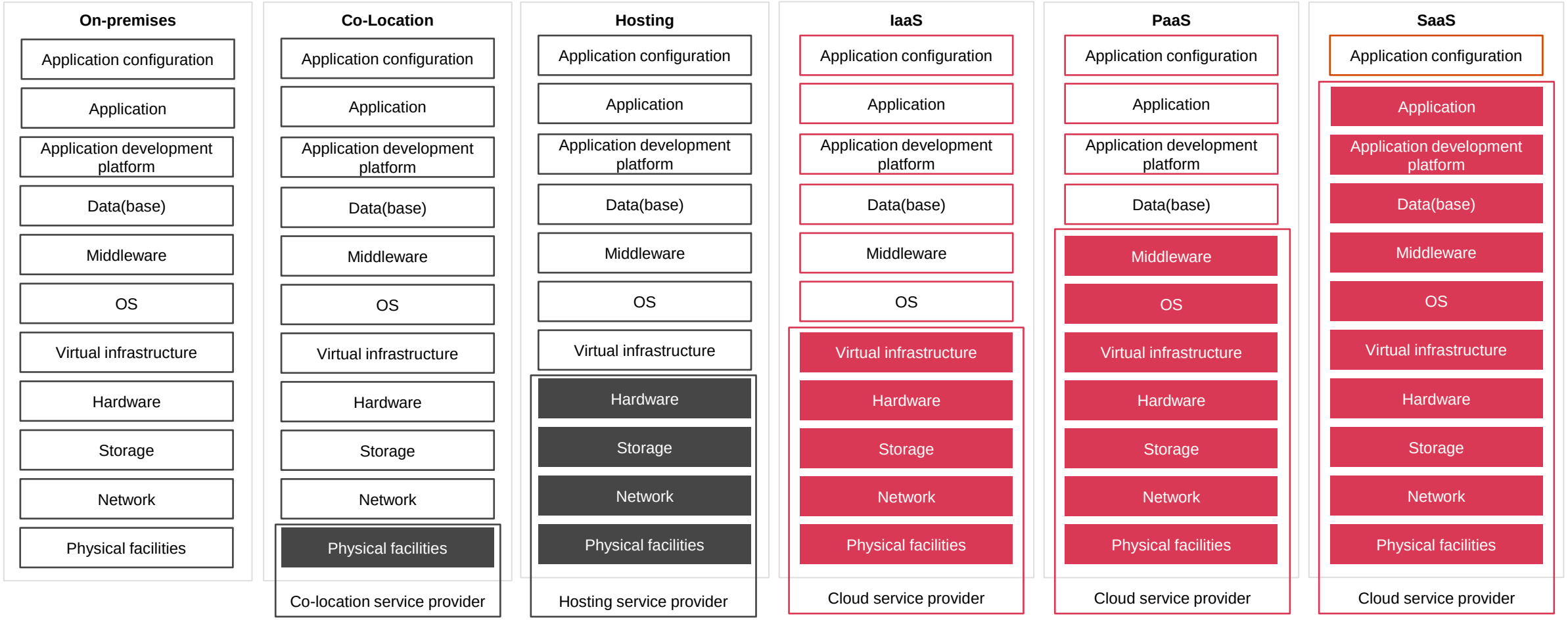
SaaS

PaaS

BPaaS

Cloud services – Shared responsibility model

Cloud services shared responsibility models



3. Cloud Integrity

Common myths about cloud compliance & security

Myths	Reality
If my cloud service provider is compliant, I am compliant.	Companies need to be ready to manage their shared responsibilities with their cloud service provider (CSP). In addition to the CSP's service auditor report (SOC), organizations must establish and maintain their own controls addressing the SOC CUECs (Complementary User Entity Controls). For organizations running IaaS or PaaS solutions, their responsibilities for company-specific controls increases (vs. SaaS).
Existing controls can be lifted and shifted.	There is not one template or one-size-fits-all approach for address cloud risk. The risks and corresponding control activities will be different and unique based on your organization's: 1. business/industry; 2. business processes on the cloud; and 3. your selection of CSP(s).

Common myths about cloud compliance & security

Myths	Reality
My existing risk management and governance programs are robust enough to tackle the cloud.	New requirements, applications cloud services and tools are introduced frequently in an ever-changing environment. Without the right governance and operating model, it can be difficult for an organization to manage its cloud risk & compliance objectives at the velocity and volume of change that occurs in the cloud.
Cloud compliance is just IT General Controls (ITGCs).	Not exactly. If you understand ITGCs, you will understand the risks associated with having your IT infrastructure in the cloud; however, each cloud provider has different infrastructure, services and tools that: 1. Need to be understand and assessed for specific risk(s) 2. Present opportunities to automate controls in the cloud (cloud policy, configuration) 3. Present opportunities to drive efficiency utilizing cloud native technology

Cloud environments present unique risks and threats

Cloud environments break the mold with dynamic new possibilities. This potential brings unique challenges, risks and threats.

4. Our Audit Approach

Combination of different types of trust services

Short Introduction

ISAE 3402

- standard for service organizations to demonstrate the design/ operation effectiveness of **their internal controls**
- report provides assurance to users of the service organization's services regarding the reliability of the controls in place
- **Predefined reporting structure**

ISAE 3000

- standard for assurance engagements on **non-financial information**
- report provides assurance on subjects such as corporate governance, risk management, sustainability reporting
- prerequisite is a type of framework with criteria against which the testing can be conducted

ISO 9001

- globally recognized standard for **quality management systems**
- valid for a specified period of time (e.g. 3 years)

ISO 27001

- globally recognized standard for **information security management systems**

SOC 1

- US standard for reporting on the controls at a service organization
- focused on controls for **financial reporting**

SOC 2

- US standard with focus on controls related to **security, availability, confidentiality, and privacy of data**

SOC 3

- summary of the controls, usually in a **less detailed format**, suitable for sharing with a broader audience

Difference between Type I and Type II

Type I: This report describes the service organization's controls at a specific point in time and assesses whether those controls are **suitably designed** to achieve the related control objectives.
Type II: This report not only includes the description of controls but also provides assurance on the **operating effectiveness** of those controls over a period of time, usually a minimum of six months.

Thank you!

pwc.at