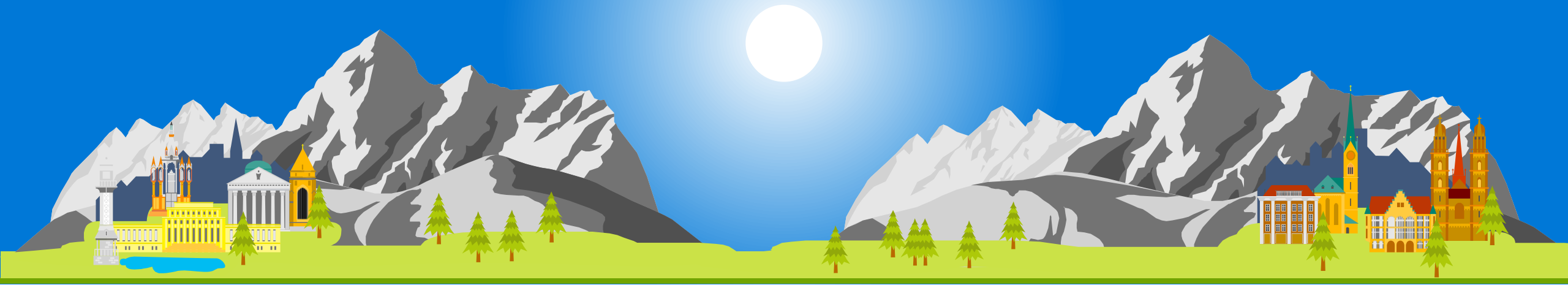


Learning Path Compliance and Privacy



Modern Cloud Risk Assessment

Dr. Marc Holitscher, National Technology Officer, Member of the Board, Microsoft Switzerland

Why Cloud?



Cloud comes with multiple benefits, most important and disruptive are the business enabling ones, allowing businesses to transform and to create new services and markets.



NEW REVENUES AND INNOVATION

- **Dynamic environment, global reach and openness** to partners
- It is the place where disruptive **innovation is happening**

ENABLE BUSINESS AGILITY

- Enable the bank **to response rapidly**
- Easier access to **new markets**

ENHANCE CUSTOMER EXPERIENCE & MOBILITY

- **Self-service**, putting **user experience** at its core
- Services are **more flexible** to changes and **easier to adopt**

COST TRANSPARENCY AND FLEXIBILITY

- Cost **transparency and the ability to steer**
- **Agility increases to scale** and address temporary needs

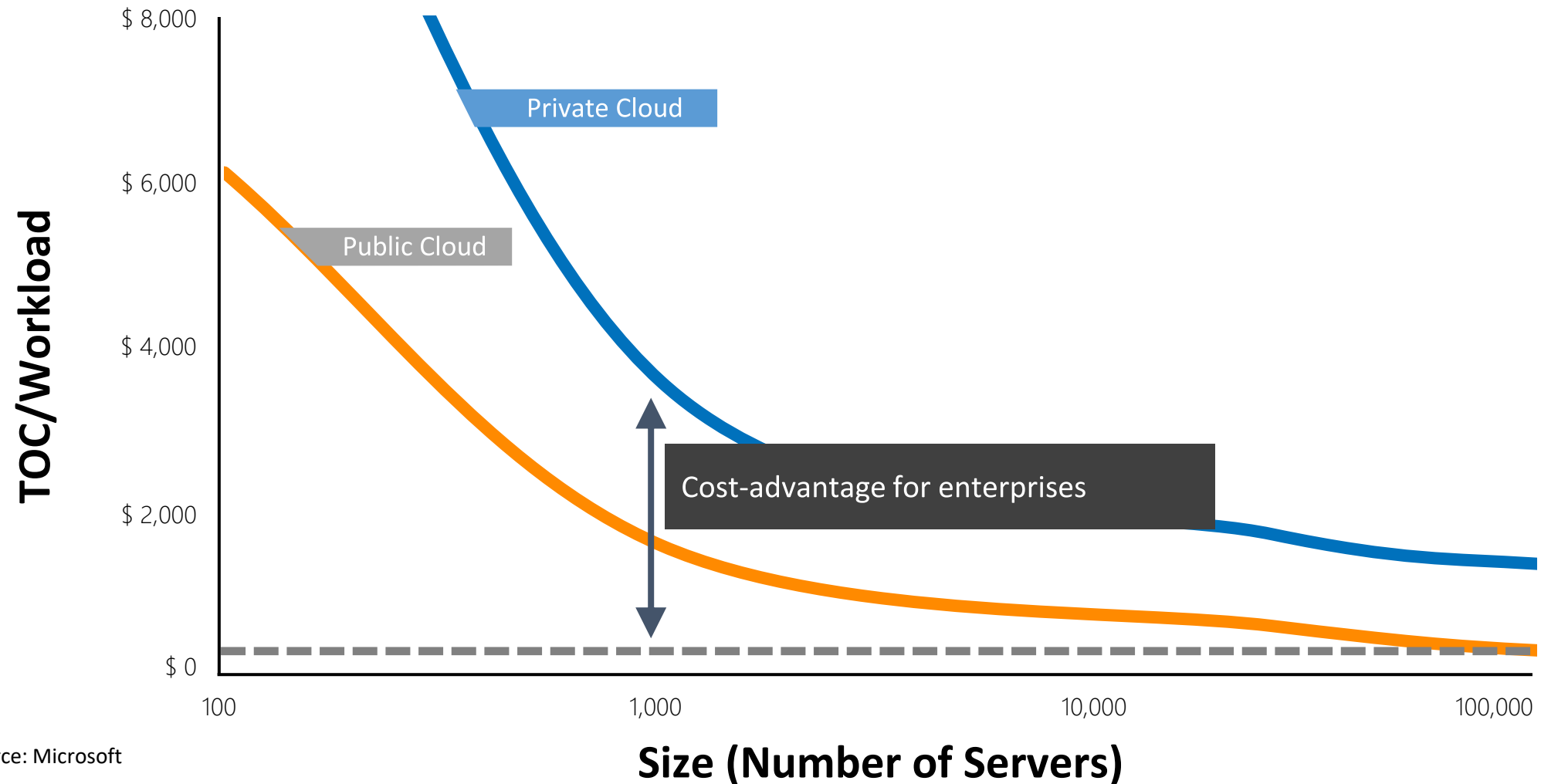
SECURITY

- **Data confidentiality** and **data recoverability** management
- **Continuous updates** of security patches and estate-wide **data encryption**
- Ability to apply **Controls**, leveraging highly **mature tooling**





Economies of Scale



Source: Microsoft

Industrialization of IT

3 key benefits:

- 1) Better Economies of Scale per Unit of IT (~10x)
- 2) Better Economics of Compliancy (~100x)
- 3) Increased Speed of Innovation (~1000x)

Note: The numbers are scale indicators



Why?

How?

Technology

Organization

Legal & regulatory
requirements



Spotlights

- Where is the data stored? What are the data flows?
- Who has access to the data? How can I determine if and how the data is accessed?
- How is the data deleted after I leave the service? Exit planning?
- What are the Service Level Agreements?
- Right to audit?
- How are Subcontractors selected?
- What happens if there is a security incident?
- How is Business Continuity implemented?
- What are possibilities for law enforcement agencies to access data?
-

Layers of risk assurance

Contractual commitments

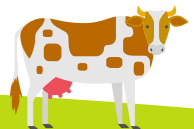
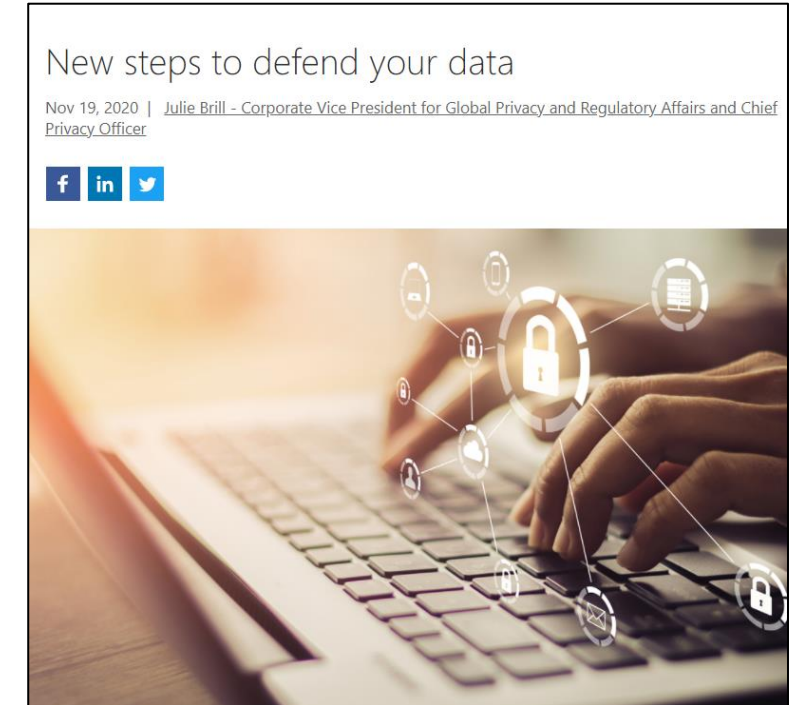
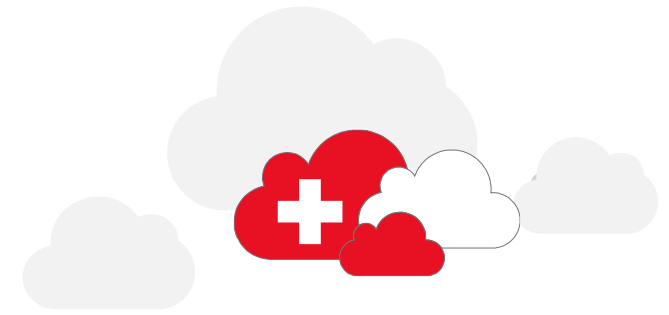
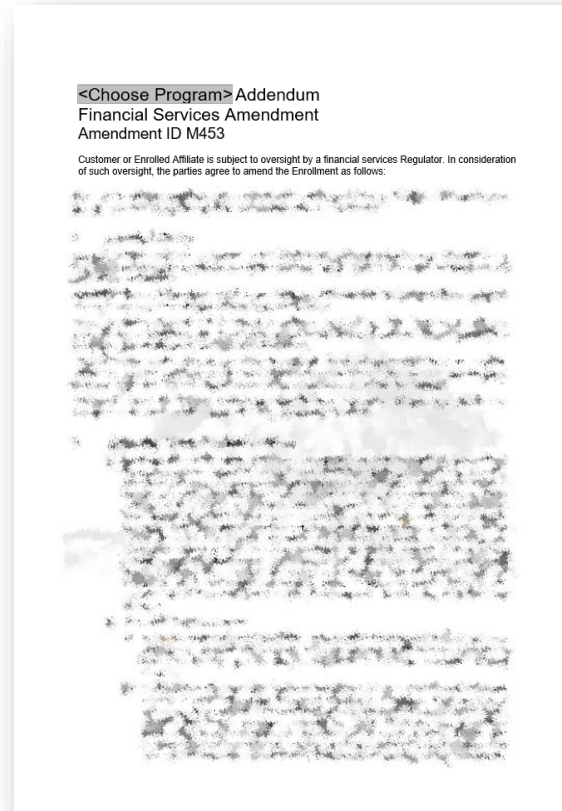
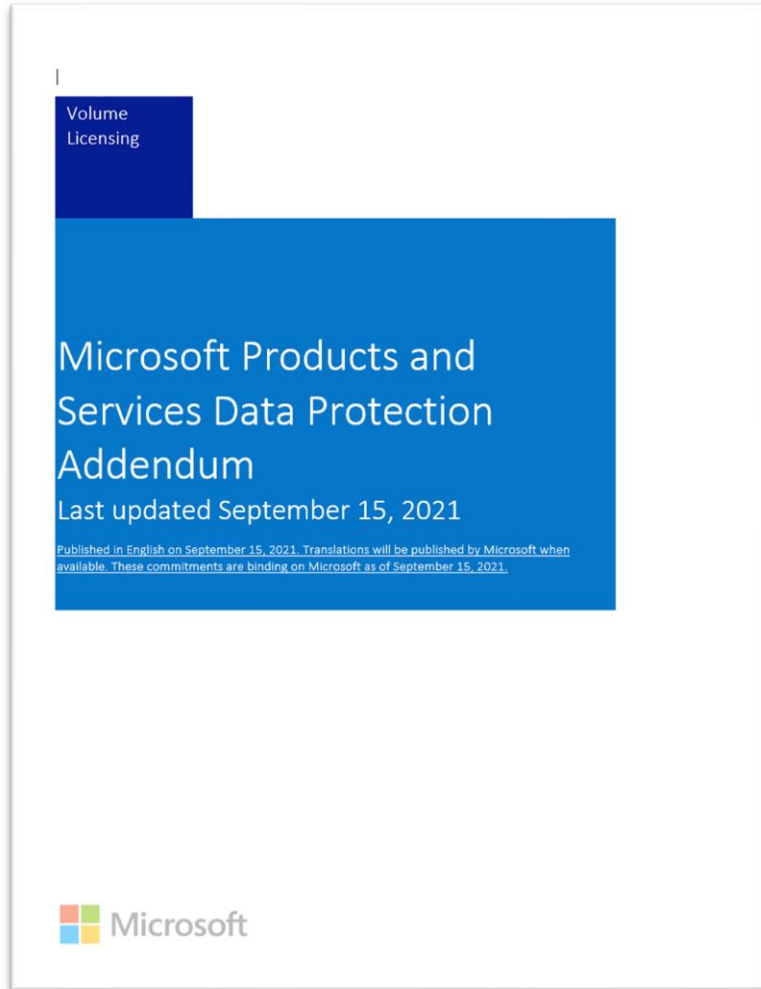
Control framework

Regulator engagement

Operating model

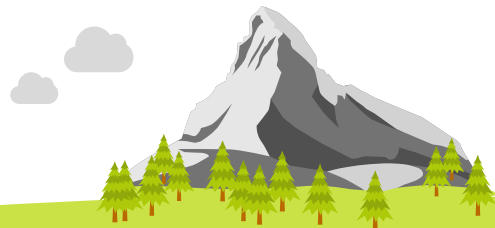


Contractual commitments



Principled approach

- We do not provide any government with direct and unfettered access to customer data.
- We do not provide any government with the ability to break encryption.
- We do not provide the government with encryption keys.
- Microsoft does comply with applicable law. A demand must follow applicable legal process.
- Microsoft only responds to requests for specific accounts/identifiers.
- Microsoft does review every legal demand to ensure it is valid.
- Privacy is a fundamental human right.



Home › Knowledge › Blog

US CLOUD Act: Why it should not prevent cloud projects

3 August 2020

Share: 

A lot of negative publicity for the US CLOUD Act

Cloud-based solutions are already widely used today, but now also companies and government agencies with "sensitive" data want to move to the cloud and use offerings such as "Microsoft 365". Interestingly enough, when planning such a move, it is not traditional data security or "business continuity" issues that seem to cause the most worry but rather the possibility of access to data by foreign authorities, particularly under the US CLOUD Act. Recently, the Zurich data protection commissioner even publicly warned public authorities against using Microsoft cloud solutions and strongly recommended the use of encryption techniques that are often hard to implement in a reasonable manner. In response, Microsoft and its lawyers are countering with legal opinions and publications.



[US CLOUD Act: Why it should not prevent cloud projects - VISCHER](#)

Deloitte.



Azure coming soon!

Microsoft (Schweiz) GmbH

Office 365 cloud services for Swiss banking clients

ISAE 3000

8 Oct 2018



BÜRO ZÜRICH
A Seegartenstrasse 2
P.O. Box 360 · CH 8024 Zürich
T +41 44 880 2424
F +41 44 880 2425
W www.lauxlawyers.ch

BÜRO BASEL
A Steinenstrasse 40 · CH 4051 Basel
T +41 61 283 0606
W www.lauxlawyers.ch

RECHTSANWÄLTE
Z Dr. Christian Laux · LL.M.
Z Dr. Jürg Hess · MBA · M.C.J.
Z Alexander Hofmann
B Mark Schieweck

In den zuständigen
Anwaltsregistern eingetragen

Rechtsgutachten

Nutzung von Cloud-Angeboten durch Banken: Zur Zulässigkeit nach Art. 47 BankG

zugleich ein Diskussionsbeitrag aus Anlass der Publikation
eines Cloud-Leitfadens der Schweizerischen Bankiervereinigung (SBVg)
zum Einsatz von Cloud-Dienstleistungen
durch Banken und Effektenhändler

Autoren:
Dr. Christian Laux
Alexander Hofmann
Mark Schieweck
Dr. Jürg Hess

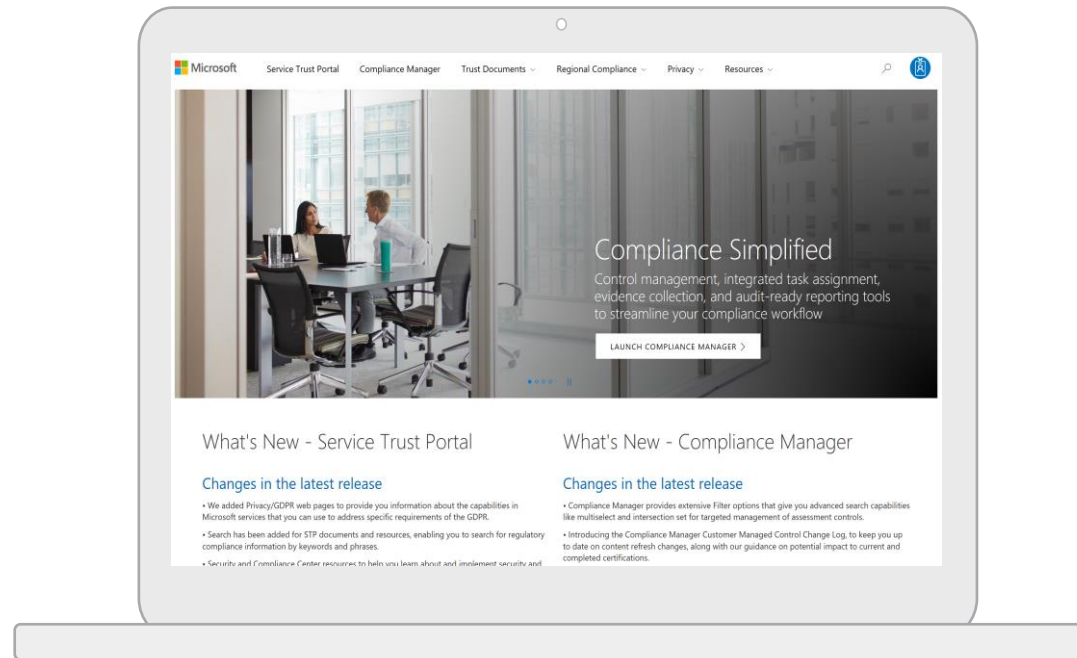
Zürich, 14. Februar 2019

Microsoft Cloud Compendium
Questions and Answers

Compliance in the Microsoft Enterprise Cloud

Published by Microsoft Switzerland Ltd Liab. Co
Version: March 2020

Control framework



<https://servicetrust.microsoft.com>

Global

- ☒ ISO 27001:2013
- ☒ ISO 27017:2015
- ☒ ISO 27018:2014
- ☒ ISO 22301:2012
- ☒ ISO 9001:2015
- ☒ ISO 20000-1:2011
- ☒ SOC 1 Type 2
- ☒ SOC 2 Type 2
- ☒ SOC 3
- ☒ CSA STAR Certification
- ☒ CSA STAR Attestation
- ☒ CSA STAR Self-Assessment
- ☒ WCAG 2.0 (ISO 40500:2012)

US Gov

- ☒ FedRAMP High
- ☒ FedRAMP Moderate
- ☒ EAR
- ☒ DFARS
- ☒ DoD DISA SRG Level 5
- ☒ DoD DISA SRG Level 4
- ☒ DoD DISA SRG Level 2
- ☒ DoE 10 CFR Part 810
- ☒ NIST SP 800-171
- ☒ NIST CSF
- ☒ Section 508 VPATs
- ☒ FIPS 140-2
- ☒ ITAR
- ☒ CJIS
- ☒ IRS 1075

Industry

- ☒ PCI DSS Level 1
- ☒ GLBA
- ☒ FFIEC
- ☒ Shared Assessments
- ☒ FISC (Japan)
- ☒ APRA (Australia)
- ☒ FCA (UK)
- ☒ MAS + ABS (Singapore)
- ☒ 23 NYCRR 500
- ☒ HIPAA BAA
- ☒ HITRUST

Regional

- ☒ Argentina PDPA
- ☒ Australia IRAP Unclassified
- ☒ Australia IRAP PROTECTED
- ☒ Canada Privacy Laws
- ☒ China GB 18030:2005
- ☒ China DJCP (MLPS) Level 3
- ☒ China TRUCS / CCCPPF
- ☒ EN 301 549
- ☒ EU ENISA IAF
- ☒ EU Model Clauses
- ☒ EU – US Privacy Shield
- ☒ GDPR
- ☒ Germany C5
- ☒ Germany IT-Grundschutz workbook
- ☒ India MeitY
- ☒ Japan CS Mark Gold
- ☒ Japan My Number Act
- ☒ Netherlands BIR 2012
- ☒ New Zealand Gov CC Framework
- ☒ Singapore MTCS Level 3
- ☒ Spain ENS
- ☒ Spain DPA
- ☒ UK Cyber Essentials Plus
- ☒ UK G-Cloud
- ☒ UK PASF

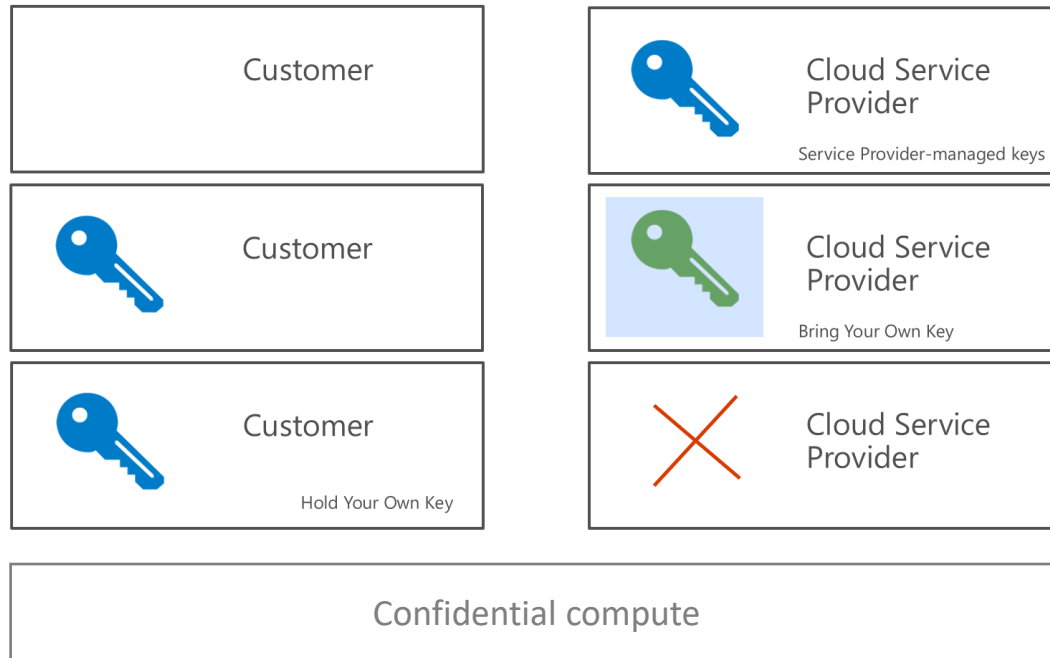
Industry

- ☒ 21 CFR Part 11 (GxP)
- ☒ MARS-E
- ☒ NHS IG Toolkit (UK)
- ☒ NEN 7510:2011 (Netherlands)
- ☒ FERPA
- ☒ CDSA
- ☒ MPAA
- ☒ DPP (UK)
- ☒ FACT (UK)
- ☒ SOX

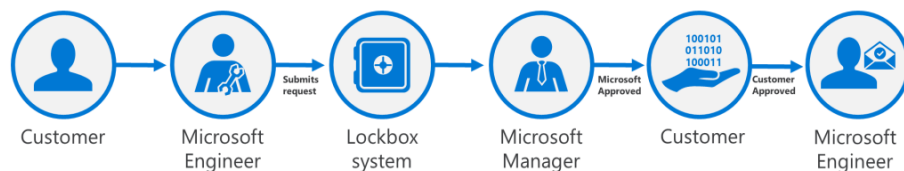
Control framework



Different flavors of encryption & key management



Zero standing access



EU data boundary

Answering Europe's Call: Storing and Processing EU Data in the EU

May 6, 2021 | [Brad Smith - President and Chief Legal Officer](#)



Today we are announcing a new pledge for the European Union. If you are a commercial or public sector customer in the EU, we will go beyond our existing data storage commitments and enable you to process and store all your data in the EU. In other words, we will not need to move your data outside the EU. This commitment will apply across all of Microsoft's core cloud services – Azure, Microsoft 365, and Dynamics 365. We are beginning work immediately on this added step, and we will complete by the end of next year the implementation of all engineering work needed to execute on it. We're calling this plan the EU Data Boundary for the Microsoft Cloud.



Regulator engagement



Canada



South Africa



Australia



Mexico



Peru



Barbados



Suriname



Vietnam



Indonesia



Ireland



Singapore



Poland



Israel



Philippines



Thailand



Dominican Rep.



Panama



Malaysia



Sri Lanka



Egypt



South Korea



UK



Greece



Hungary



Czech Rep.



Serbia



Croatia



Slovakia



Romania



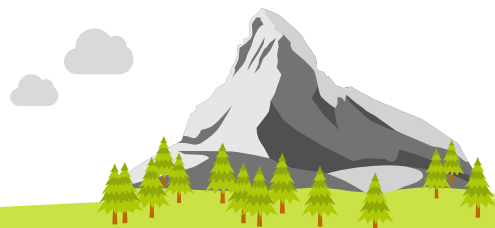
Latvia



Switzerland



Japan



Emerging Regulatory Discussions...

AI and Ethics

- New Regulation?

Cyber Risk

- Scale mitigates risk?

Concentration Risk

- How to assess and manage?

Regulating cloud vendors

- Critical infrastructure utilities?

Geopolitical Risk

- Exit and continuity planning?

Cloud Governance

- Scalable and flexible approaches

New Computing Models and Regulation

- Quantum Computing?

Microsoft Cloud in Switzerland



Compliance



Data
Residency



Performance



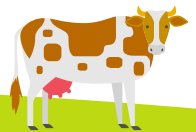
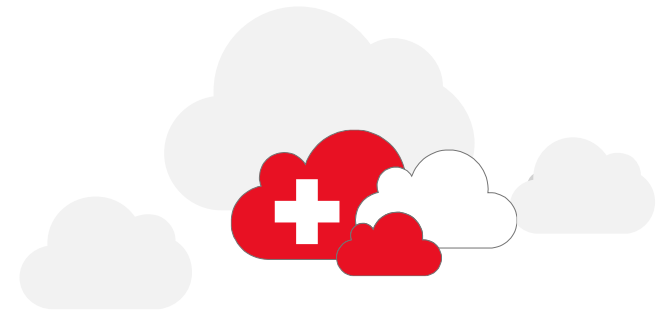
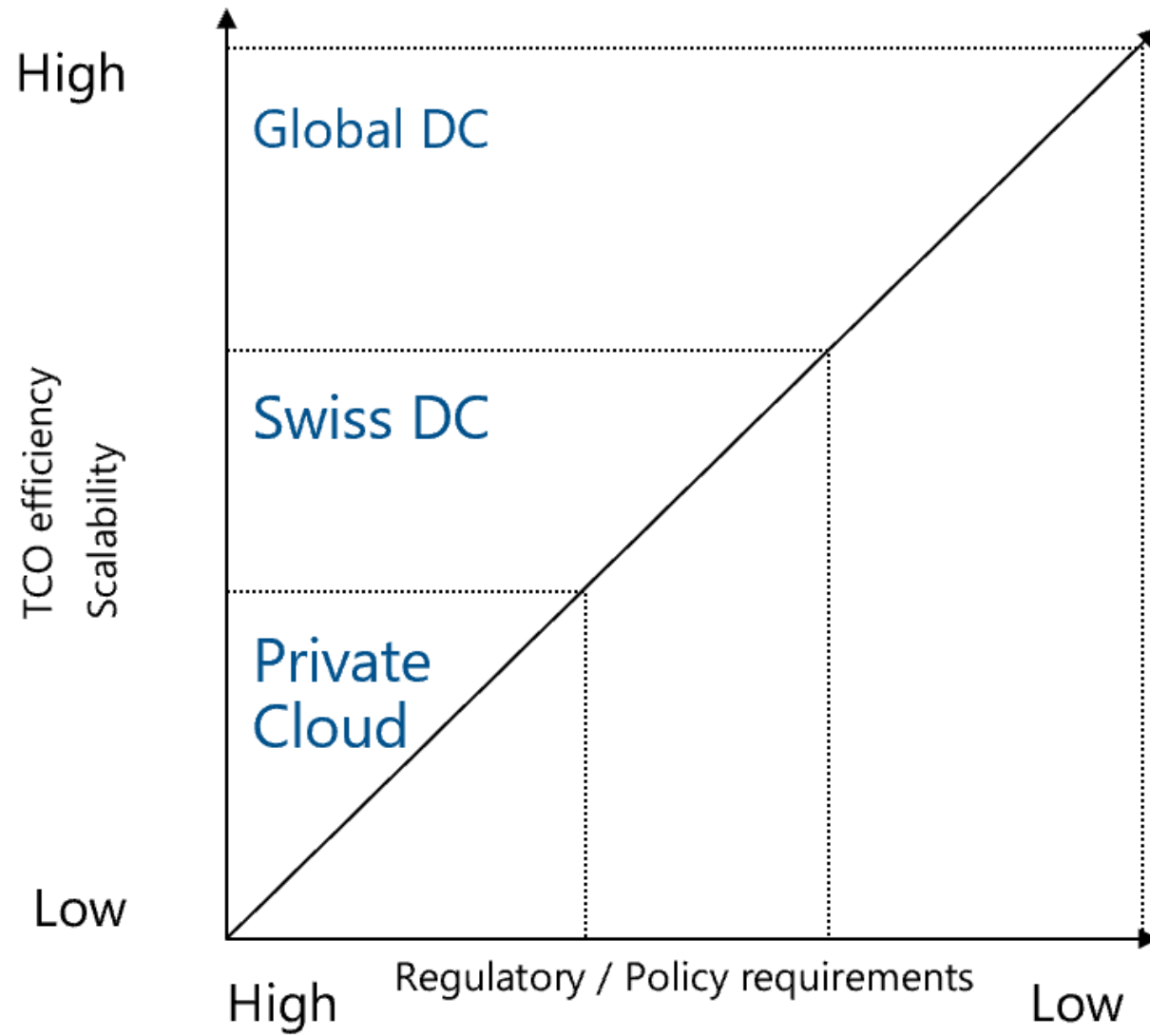
Extract of Client References and Testimonials

Clients



Solutions





Key Lessons Learned

1. Seek approval for a specific project – don't look for approval for "cloud" in general
2. Involve your internal Legal, Risk & Compliance stakeholders early in the process
3. Develop a solid Risk Assessment as a key enabling document
4. Microsoft will actively support you through the process



Microsoft