ERNW
providing security.

Sicherheit von Cloud Lösungen

Matthias Luft, mluft@ernw.de

ERNW GmbH

Heidelberg based security consulting and assessment company.

- Independent
- We understand corporate
- Deep technical knowledge
- Structured (assessment) approach
- Business reasonable recommendations

- Blog: www.insinuator.net
- Conference: www.troopers.de

ERNW

ERNW provides vendor independent security services to support our customers' business.

- Established 2001
- 42 employees
- Customers predominantly large/very large enterprises
  - Industry, telecommunications, finance

Agenda

- Definition
- Security Incidents
- Regulatory Requirements
- Trust Evaluation

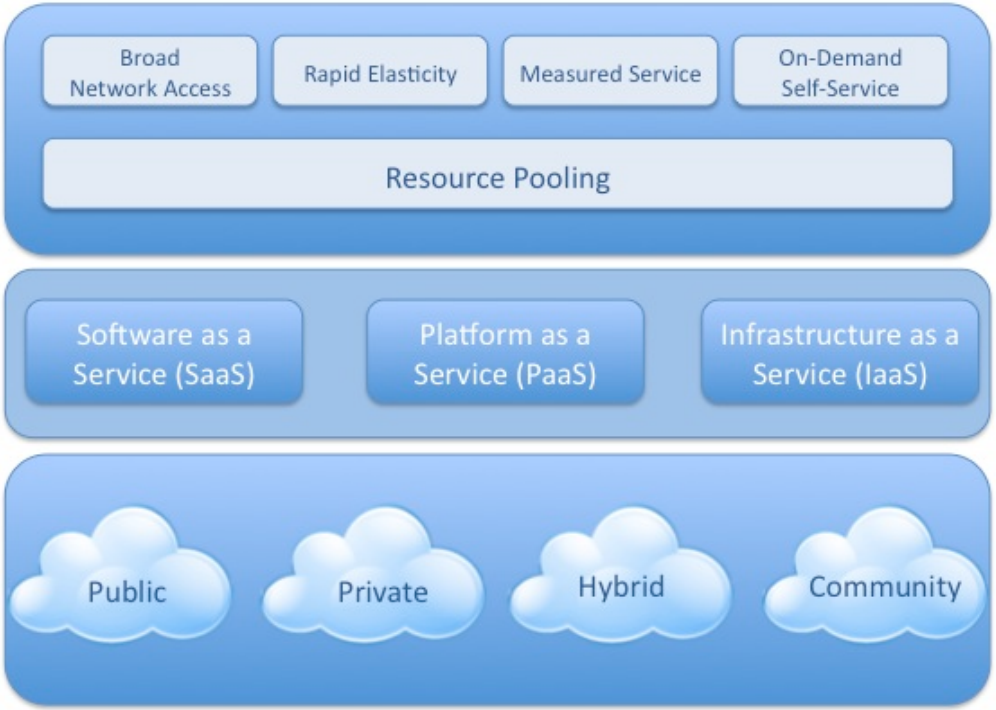
ERNW
providing security.

The Cloud?

- "Think stateless CPU in the Cloud”
- "The unique architecture of the cloud not only offers unlimited storage capacity, but also lays the groundwork for eliminating the daily grind of data backup thanks to the cloud’s constant replication of data."

Definition of Cloud computing

Visual Model Of NIST Working Definition Of Cloud Computing
http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



Essential Characteristics

Service Models

Deployment Models

ERNW
providing security.

Relevant Characteristics

- Multi Tenancy
- Self-Service & High Degree of Automation
- Restricted Contractual Options

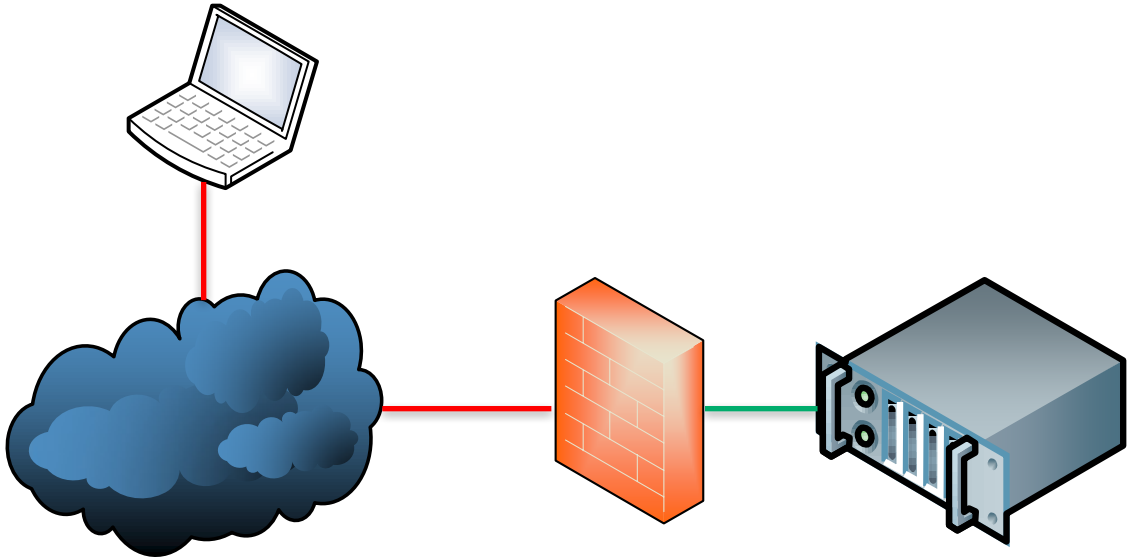
Distinction

	Multi Tenancy	Self Service	Contractual Restrictions
Public Cloud	✔	✔	✔
Outsourcing	✔	✔	
Private Cloud	✔		

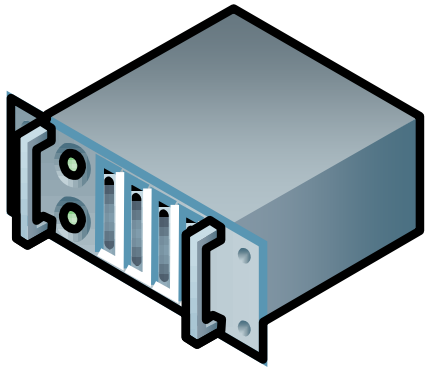
Security Concerns

- “Where is my data stored?”
- “Who has access?”
- “Do I have to take care of backups?”
- “Is the service secure?”
- “Can I be compliant in the cloud?”

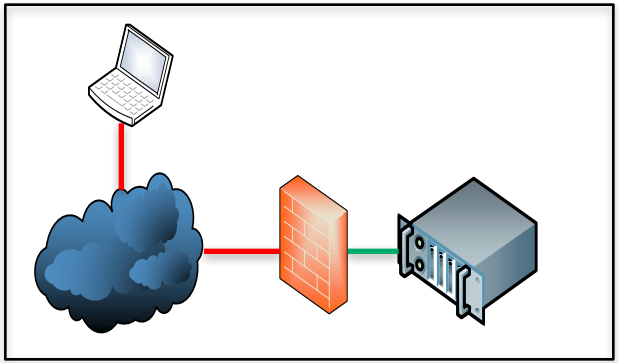
The (really) old World

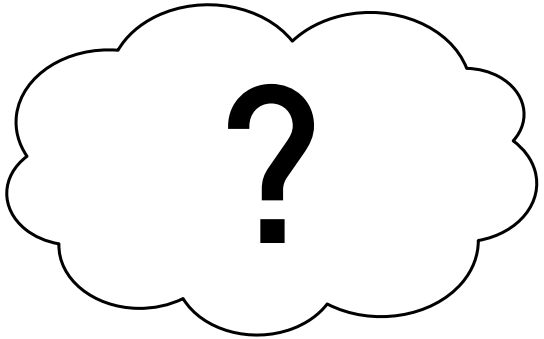


The new Virtualized World



The new Cloud World





There Is No Cloud

- There are many clouds.
- There is no cloud technology.
- A Cloud is a composition of
  - Hardware
    - Processors, RAM, Disks, Network
  - Technologies
    - Virtualization
    - Network Separation
    - Management solutions ("Scripts", "Webfrontends", APIs)
    - Storage
    - Programming APIs
  - "Glue code"

ERNW
providing security.

Security Incidents

Incidents

- Known data breaches of the very large Cloud Providers (e.g. Amazon, Microsoft, Google): Zero.
- However, there are a number of known vulnerabilities/incidents:
  - Web application/service vulnerabilities
  - Operational mistakes/human error

Data Protection/Personal Data

Personal Data

- [EU_DIR]: any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

Personal Data

- [BDSG]: “Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“.

→ Essentially, this means: all data related to a *person*.

Control of processing in foreign countries

- [BDSG, § 4b]: “Übermittlung personenbezogener Daten ins Ausland”
- Transfer to member states of EU or EEA
  permissible without any additional requirements.
- For other countries, see next slide.

Control of processing in foreign countries

- Transfer to/processing in Non-EU Countries:
  - For the USA:
    - Until 10/2015: Safe Harbor
    - 10/2015-02/2016: Safe Harbor was declared invalid, transfer to the US illegal.
    - From 02/2016 on: EU-US Privacy Shield
      - Details still to be finalized.
  - For other countries:
    - Use of EU Standard Contractual Clauses

Control of processing in foreign countries

- Question: If the data is stored in the AWS datacenter in Frankfurt, is is still processing in foreign countries?
- Answer:
  - As of 02/2016, situation still not clear.
    - US agencies have access to this data, by court order.
    - Microsoft appealed to this ruling.
  - If the ruling keeps in place, a datacenter in the EU of a US company means processing in foreign country:
    - The CP has to ensure that the data is not leaving the EU.

Control of processing by 3rd parties

- "Auftragsdatenverarbeitung"
- [BGSG, §11]: "Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag"

  "Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der **Auftraggeber** für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich."

  → You can't transfer (your) responsibility.

  "Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen".

  → The contract is important! See [BDSG, § 11] for details.

- Prerequisites for processing personal data in the cloud:
  - Contract covering Auftragsdatenverarbeitung/Einhaltung technischer und organisatorischer Maßnahmen
  - Restrict processing to EU countires, make sure that EU Standard Contractual Clauses are in place, or make sure that CP is covered by the EU-US Privacy Shield.

Sources

- https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf
- https://www.datenschutzbeauftragter-info.de/fachbeitraege/auftragsdatenverarbeitung/
- https://www.datenschutzbeauftragter-info.de/berufungsverfahren-microsoft-streitet-fuer-datenschutz-der-cloud/
- https://www.datenschutzbeauftragter-info.de/auftragsdatenverarbeitung-was-sind-eu-standardvertragsklauseln/
- https://www.datenschutzbeauftragter-info.de/eu-us-privacy-shield-eine-verbesserung-fuer-unternehmen-und-buerger/
- http://europa.eu/rapid/press-release_IP-16-216_en.htm

Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures

Version 2.0

October 2010

PCI-DSS

Overview

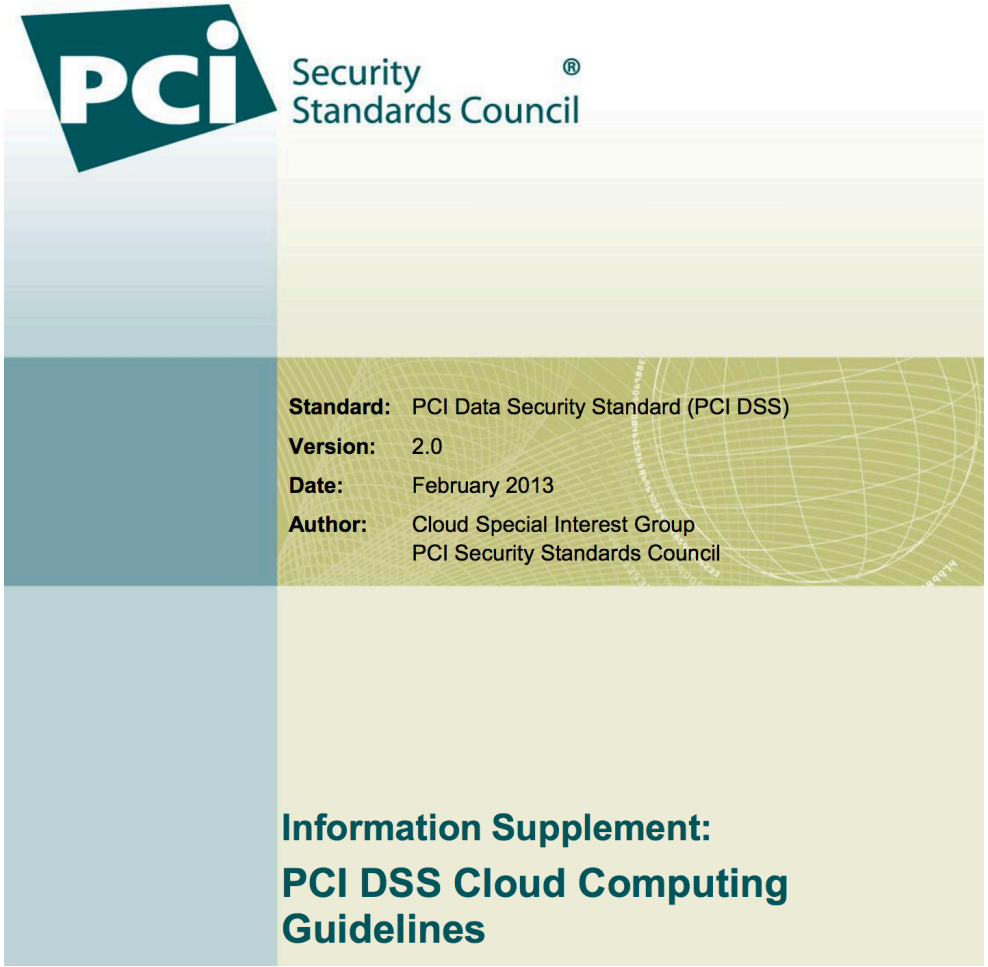
- In the past achieving PCI compliance with cc/cardholder data processing in the (public) cloud was regarded “unlikely“.
- In the interim, some CPs have taken care of this (see next slides for a sample selection)

AWS

- https://aws.amazon.com/compliance/pci-dss-level-1-faqs/:
- „The AWS services listed below and their supporting infrastructures are PCI DSS compliant. This compliance has been validated by an authorized independent Qualified Security Assessor. Conversely, PCI "certification" is a term reserved for those merchants who require certification to process credit card transactions. AWS, as a service provider, does not directly manage cardholder environments (and therefore, unlike merchants, does not require certification). AWS provides a secure environment that has been validated by a QSA, allowing merchants to establish a secure cardholder environment and to achieve their own certification, having confidence that their underlying technology infrastructure is compliant. Achieving PCI DSS 3.1 validation for AWS helps our customers obtain their own PCI certification.“

Salesforce

- https://help.salesforce.com/apex/HTViewSolution?urlname=Salesforce-PCI-Attestation-of-Compliance&language=en_US:
- “For the services branded as Force.com, Site.com, Database.com, Sales Cloud, Service Cloud, Communities, Analytics Cloud, and Chatter, Salesforce has obtained a signed Payment Card Industry Attestation of Compliance (“AoC”). This attestation demonstrates Level 1 compliance with the Payment Card Industry Data Security Standard ("PCI DSS") version 3.1, as formulated by the Payment Card Industry Security Standards Council. In order to benefit from Salesforce’s PCI AoC, customers must use either "Platform Encryption" for supported fields types or “Classic Encryption” technology available in the Services.”



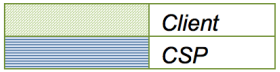
ERNW
providing security.

PCI DSS & Cloud

Summary – Only applicable for Cloud?

- It's important to note that all cloud services are not created equal. Clear policies and procedures should be agreed between client and cloud provider for all security requirements, and responsibilities for operation, management and reporting should be clearly defined and understood for each requirement.
- All PCI-DSS requirements must also be fulfilled in the Cloud Environment.

ERNW
providing security.



Cloud Layer	Service Models		
	IaaS	PaaS	SaaS
Data	Client	Client	Client
Interfaces (APIs, GUIs)	Client	Client	CSP
Applications	Client	Client	CSP
Solution Stack (Programming languages)	Client	Client	CSP
Operating Systems (OS)	Client	CSP	CSP
Virtual Machines	Client	CSP	CSP
Virtual network infrastructure	Client	CSP	CSP
Hypervisors	CSP	CSP	CSP
Processing and Memory	CSP	CSP	CSP
Data Storage (hard drives, removable disks, backups, etc.)	CSP	CSP	CSP
Network (interfaces and devices, communications infrastructure)	CSP	CSP	CSP
Physical facilities / data centers	CSP	CSP	CSP

Responsibilities

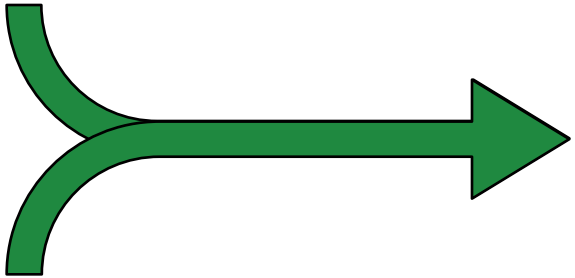
	Client
	CSP
	BOTH Client and CSP

PCI DSS Requirement	Example responsibility assignment for management of controls		
	IaaS	PaaS	SaaS
1: Install and maintain a firewall configuration to protect cardholder data	Both	Both	CSP
2: Do not use vendor-supplied defaults for system passwords and other security parameters	Both	Both	CSP
3: Protect stored cardholder data	Both	Both	CSP
4: Encrypt transmission of cardholder data across open, public networks	Client	Both	CSP
5: Use and regularly update anti-virus software or programs	Client	Both	CSP
6: Develop and maintain secure systems and applications	Both	Both	Both
7: Restrict access to cardholder data by business need to know	Both	Both	Both
8: Assign a unique ID to each person with computer access	Both	Both	Both
9: Restrict physical access to cardholder data	CSP	CSP	CSP
10: Track and monitor all access to network resources and cardholder data	Both	Both	CSP
11: Regularly test security systems and processes	Both	Both	CSP
12: Maintain a policy that addresses information security for all personnel	Both	Both	Both
PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers	CSP	CSP	CSP

Responsibilities

Trust Evaluation

TRUST



CONFIDENCE

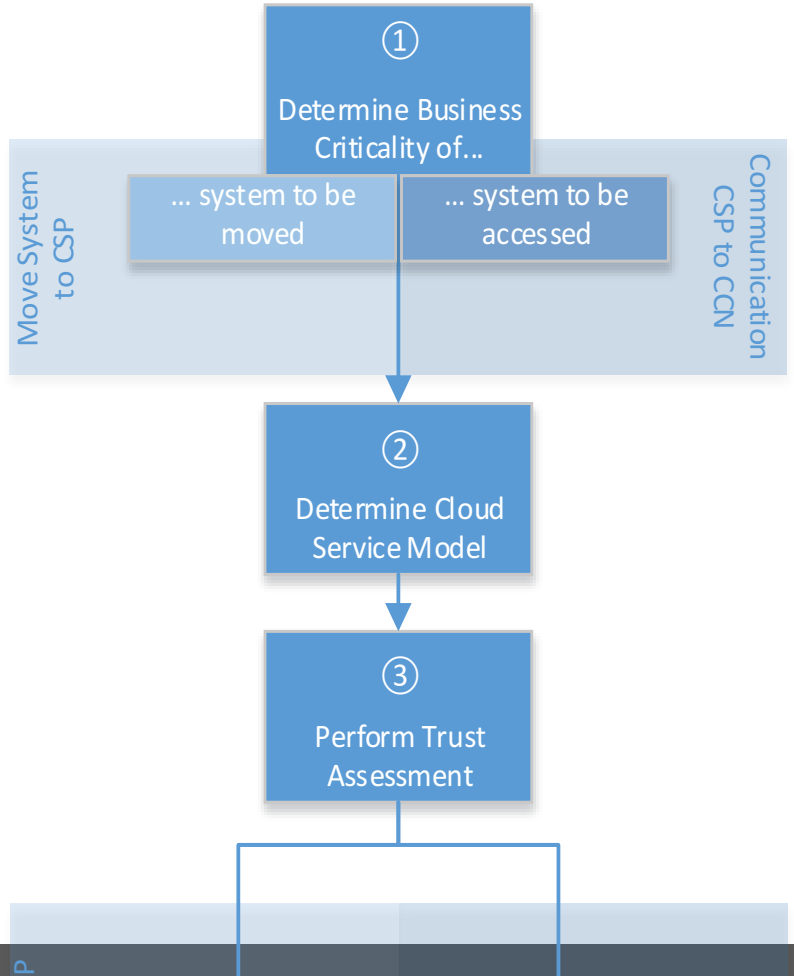
CONTROL

Back to trust

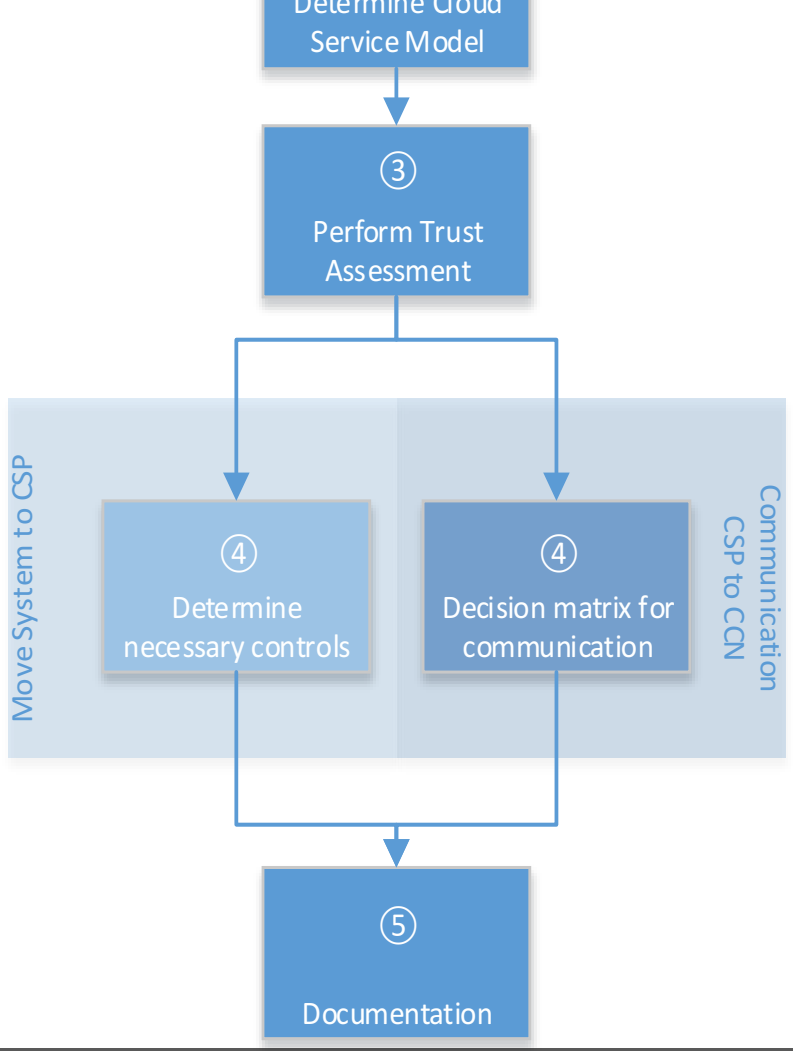
- Trust needs evidence.
  - Otherwise it would be *faith*.

Trust Factors

- Symmetry & Understanding
- Transparency
- Consistency
- Competence
- Integrity
- Components



Trust Assessment

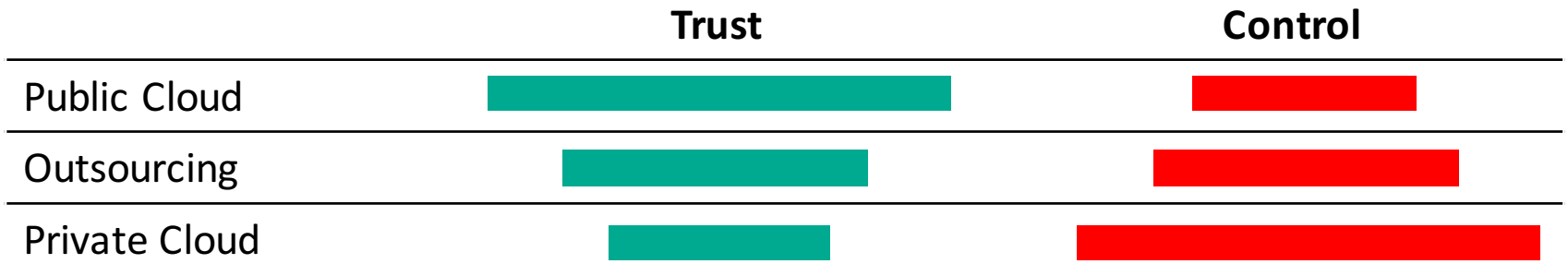


Trust Assessment

Trust or Control?

	Multi Tenancy	Self Service	Contractual Restrictions
Public Cloud	✔	✔	✔
Outsourcing	✔	✔	
Private Cloud	✔		

Trust or Control?



There's never enough time...

THANK YOU...

...for yours!

@uchi_mata

mluft@ernw.de