

# Trust Evaluation of Cloud Providers

Matthias Luft

ERNW Research GmbH





## ERNW

- Vendor-independent
- Established 2001
- 60 employees, 40 FTE consultants
- Continuous growth in revenue/profits
  - No venture/equity capital, no external financial obligations of any kind
- Customers predominantly large/very large enterprises
  - Industry, telecommunications, finance





Since 2016



## Agenda

- Cloud Security Challenges
- Gap Analysis
- Trust Evaluation



# Cloud Adoption

- Increasing!
  - Own experience: Increasing even among German companies and for production systems.
- Great Feature Set
  - Heavy orchestration and integration
  - Service discovery features
  - Supporting infrastructure “by click”



## Cloud Understanding?

- "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."





## Relevant Characteristics

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

## Security Concerns?

- 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



## Security Concerns!

- Large attack surface
  - Web interfaces & virtualization
- Security posture of web services and virtualization
- High-return target

## Do we know...

- ... which hypervisor Amazon uses?
  - ... and how it is hardened?
- ... how Azure secures their service API?
- ... whether the ISO 27000 certification covered the development of automation scripts?

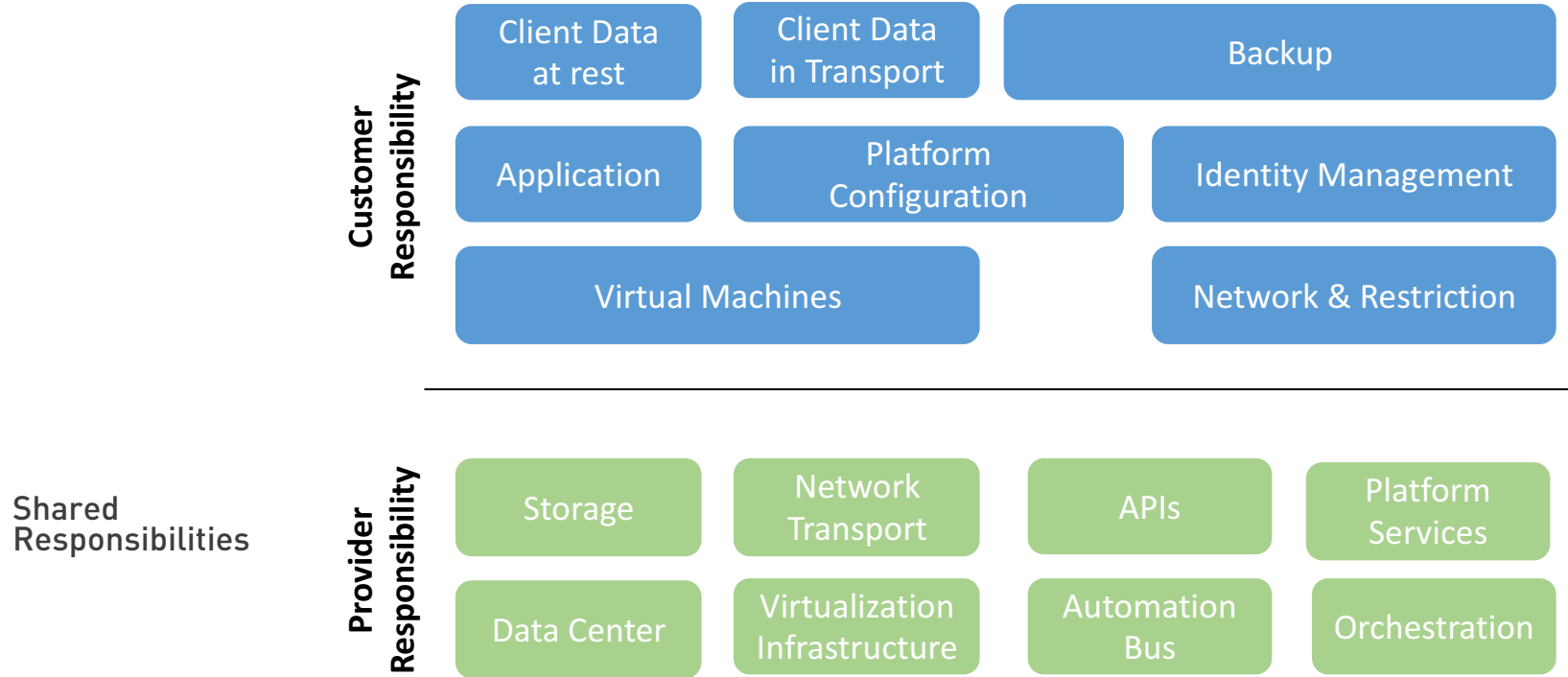




## Limitations of Technical Controls

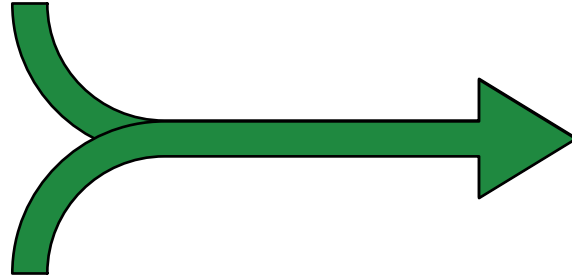
	Client
	CSP
	BOTH Client and CSP

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





TRUST



CONTROL



## Trust?

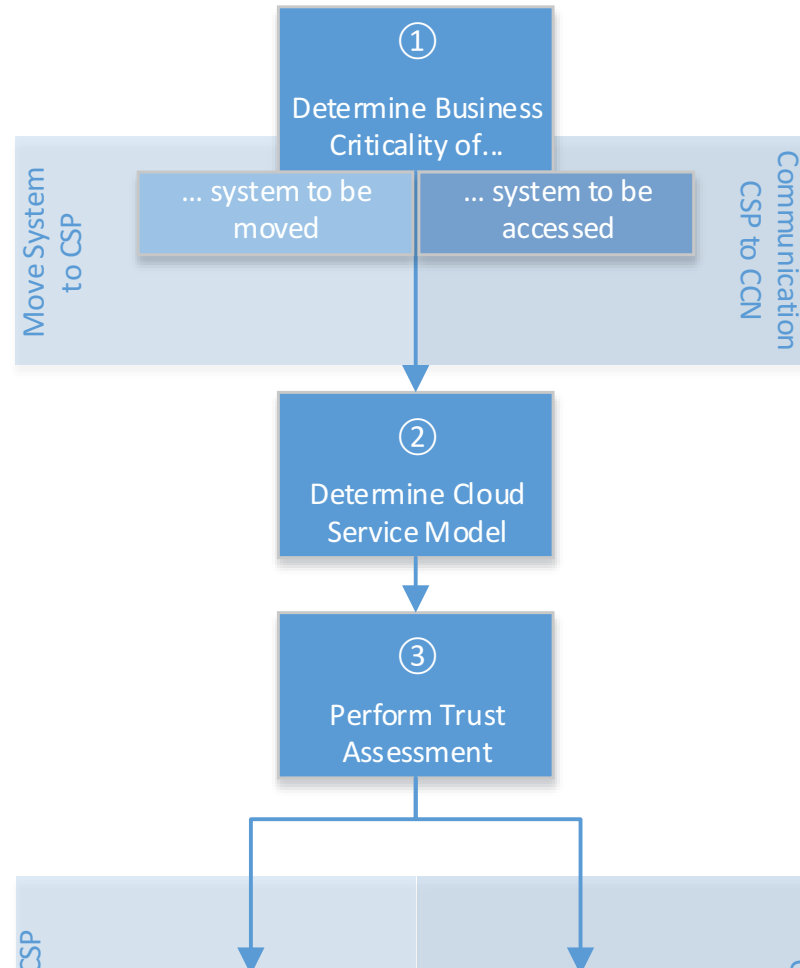
- Trust needs evidence.
- Otherwise: Faith.

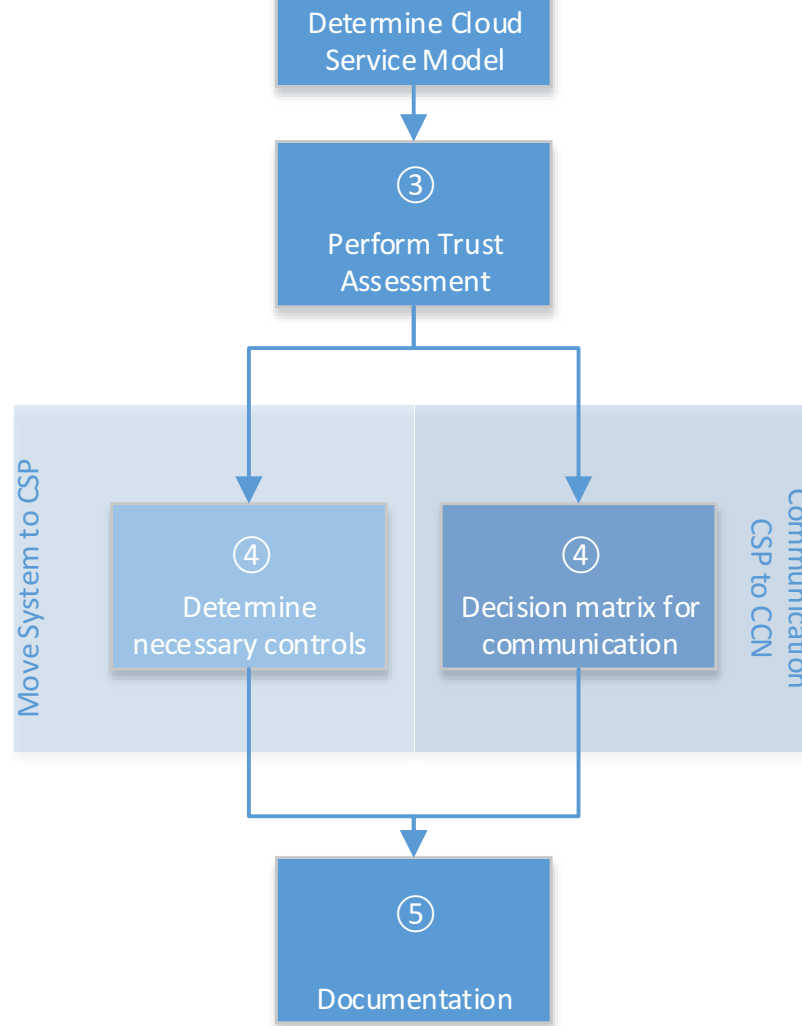










## Trust Factors

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





## Trust or Control?

	Trust	Control
Public Cloud		
Outsourcing		
Private Cloud		

## Conclusions

- Understand cloud technology
- Understand shared responsibilities
- Apply controls where you can
- ... and identify required level of Trust where you cannot





# Thank you for your Attention!

Questions?



mluft@ernw.de



@uchi\_mata



[www.ernw.de](http://www.ernw.de)



[www.insinuator.net](http://www.insinuator.net)

