PARTNERING TRUST

"Enabling trust in the digital online economy"

PARTNERING TRUST

Michiel Steltman

- Project lead, Partnering Trust
- Director, DINL
- Member, NL forum standardization

Thomas Niessen

- MD, Kompetenznetzwerk Trusted Cloud
- Managed largest German innovation programs (Internet of Services/Cloud);
- VP, software company specialized in information retrieval/Big Data.

Bianca Smit

- Certified auditor (RA),
- Examiner, Financial auditing Amsterdam University
- Lecturer Financial Accounting, Nyenrode Business University

Jeroen van Schajik

- IT audit partner, BDO Audit & Assurance
- Responsible for the NL SOC (Service Organization Control) assurance practice
- Board member, NOREA
- Involved in development Zeker Online

Partnering trust

"Enabling trust in the digital online economy"

Partnering Trust: Ambitions

Generic processing agreements

Information Security Baselines
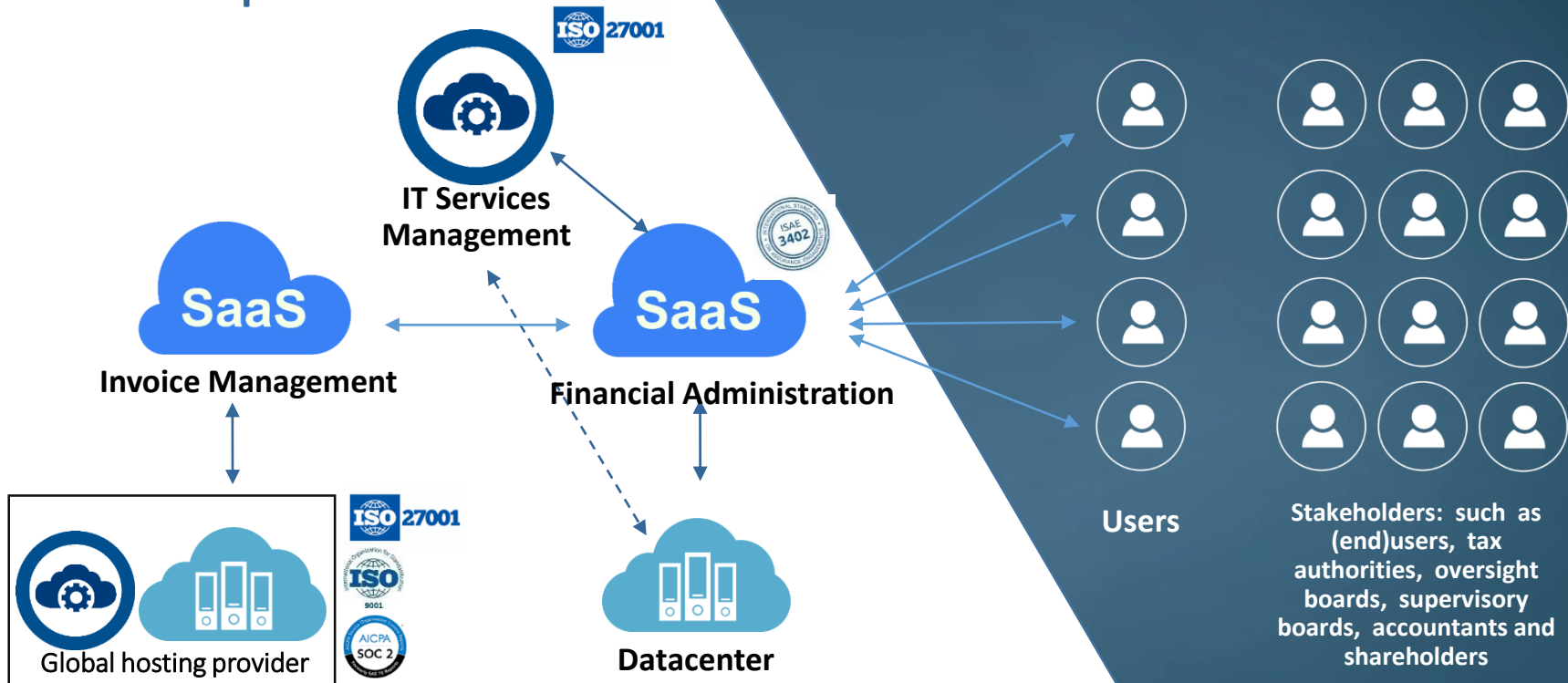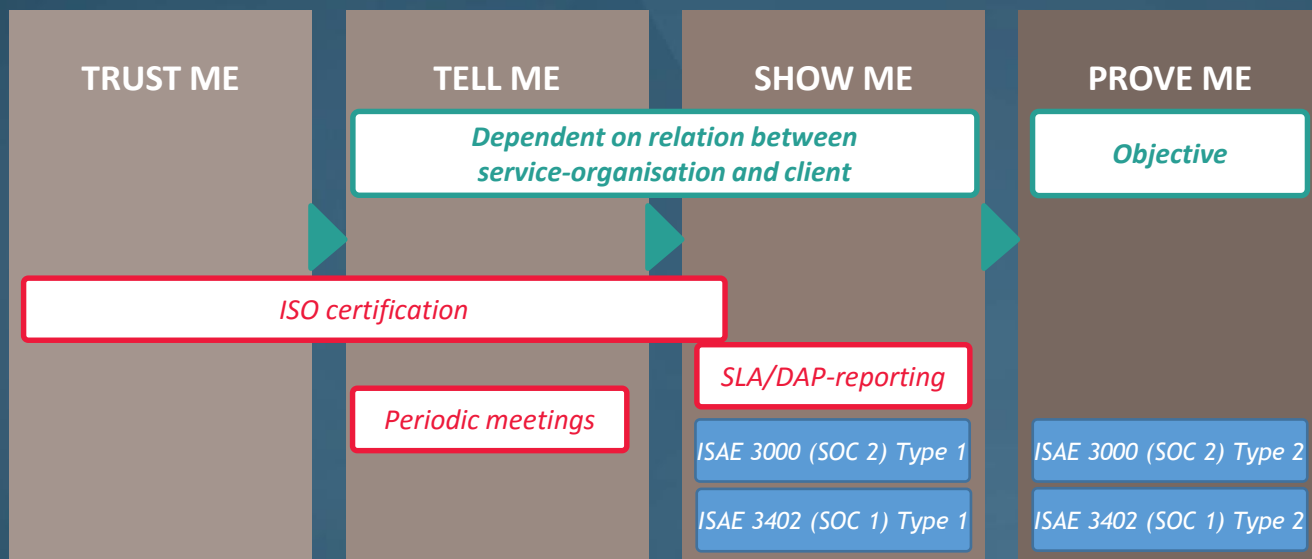
Reusable and standardized audit reports

DPA Endorsement

International Level playing field

Certification and assurance: an example

IT Services Management
ISO 27001

Invoice Management

Financial Administration
ISAE 3402

Global hosting provider
ISO 27001
ISO 9001
AICPA SOC 2

Datacenter

Users

Stakeholders: such as (end)users, tax authorities, oversight boards, supervisory boards, accountants and shareholders

Certification versus assurance reports

ISAE 3000: SOC 2 implementation

Security: 28 criteria (= baseline)

Confidentiality: 6 additional criteria

CONTROLS ❓

Availability: 3 additional criteria
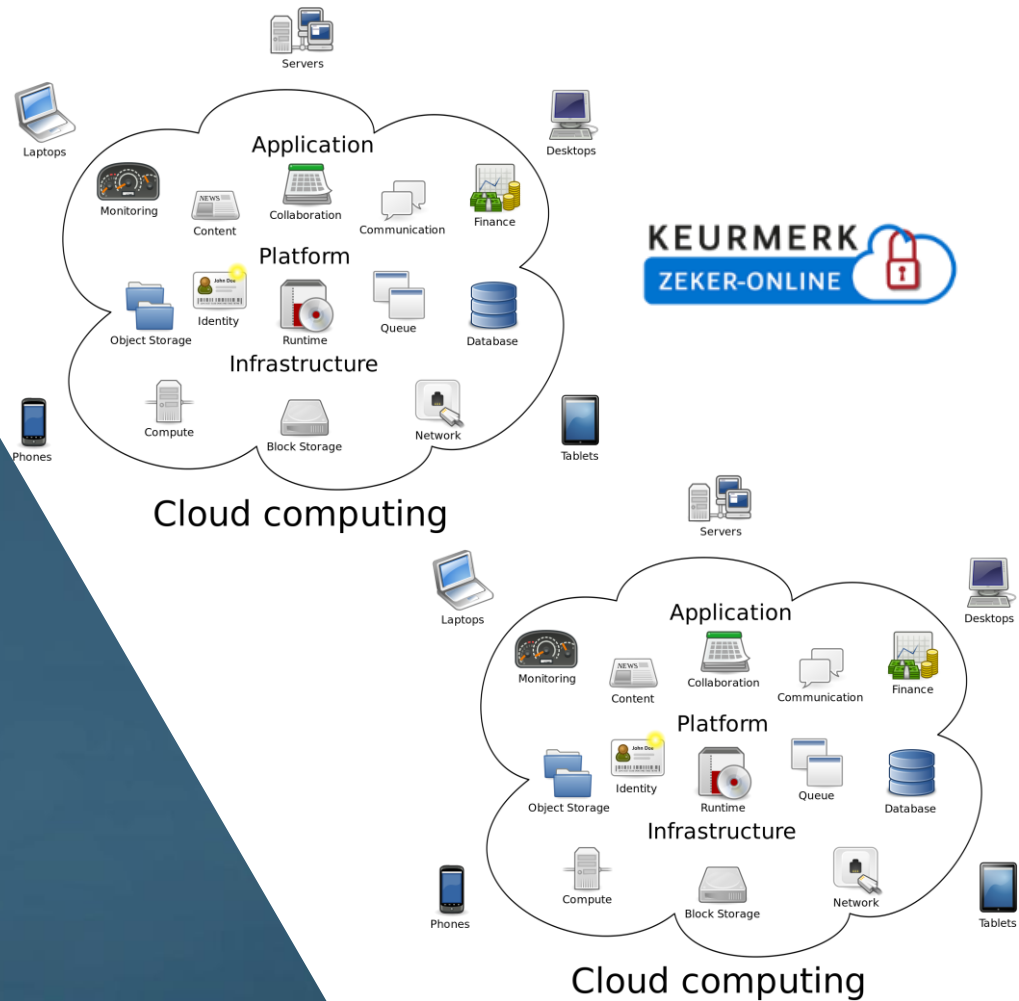
Processing integrity: 6 additional criteria

Privacy: 6 additional criteria (USA)

Frameworks with mapping to SOC 2

Quality Requirements & desired Chain

Legal Requirements

Technical Infrastructure
- IT Organization
- Security

Application Structure
- Generic
- Specific

End users

SaaS

SaaS   SaaS

PaaS

IaaS

Certification versus assurance reports

TRUST ME	TELL ME	SHOW ME	PROVE ME
	Dependent on relation between service-organisation and client		Objective
ISO certification			
	Periodic meetings	SLA/DAP-reporting	
		ISAE 3000 (SOC 2) Type 1	ISAE 3000 (SOC 2) Type 2
		ISAE 3402 (SOC 1) Type 1	ISAE 3402 (SOC 1) Type 2

Community

Supervisory board
- Adopt of the framework

Stichting Zeker-Online
- Grantor of the certification

Participant Council
- Advise

Workgroup Auditors

Standard Setting Cie

Summary

- **Initiative of innovative players**
- **Pro-active in the new data-economy**
- **Market demand for 'trusted' online services**
- **Data protection, privacy**
- **Cooperation between government and industry**
- **Demand for independent 'assurance' providing**
- **SAAS- PAAS – IAAS - …… Chain security !!**

Trusted Cloud Label

Cloud provider applies → **External auditor examines the application** → **Advisory Board makes decision on application** → **Label is awarded, service is listed**

Stakeholders:

bitkom

bvmw Bundesverband IT-Mittelstand e.V.

VOICE CIO Bundesverband der IT-Anwender e.V.

EuroCloud DEUTSCHLAND | eco

Bundesministerium für Wirtschaft und Energie

Criteria of Trusted Cloud Label

Service Management

Data Privacy / Protection

Flexibility

Quality

Trans parency

Continuity Management

Security Aspects

Aims of co-operation

Trusted Cloud

KEURMERK ZEKER-ONLINE

LABEL CLOUD

Harmonization of the existing labels

- Common criteria
- Criteria for special target groups
- Processes to apply for a label
- Identify best practices

All labels ensure:

Increasing confidence in cloud computing (security aspect)

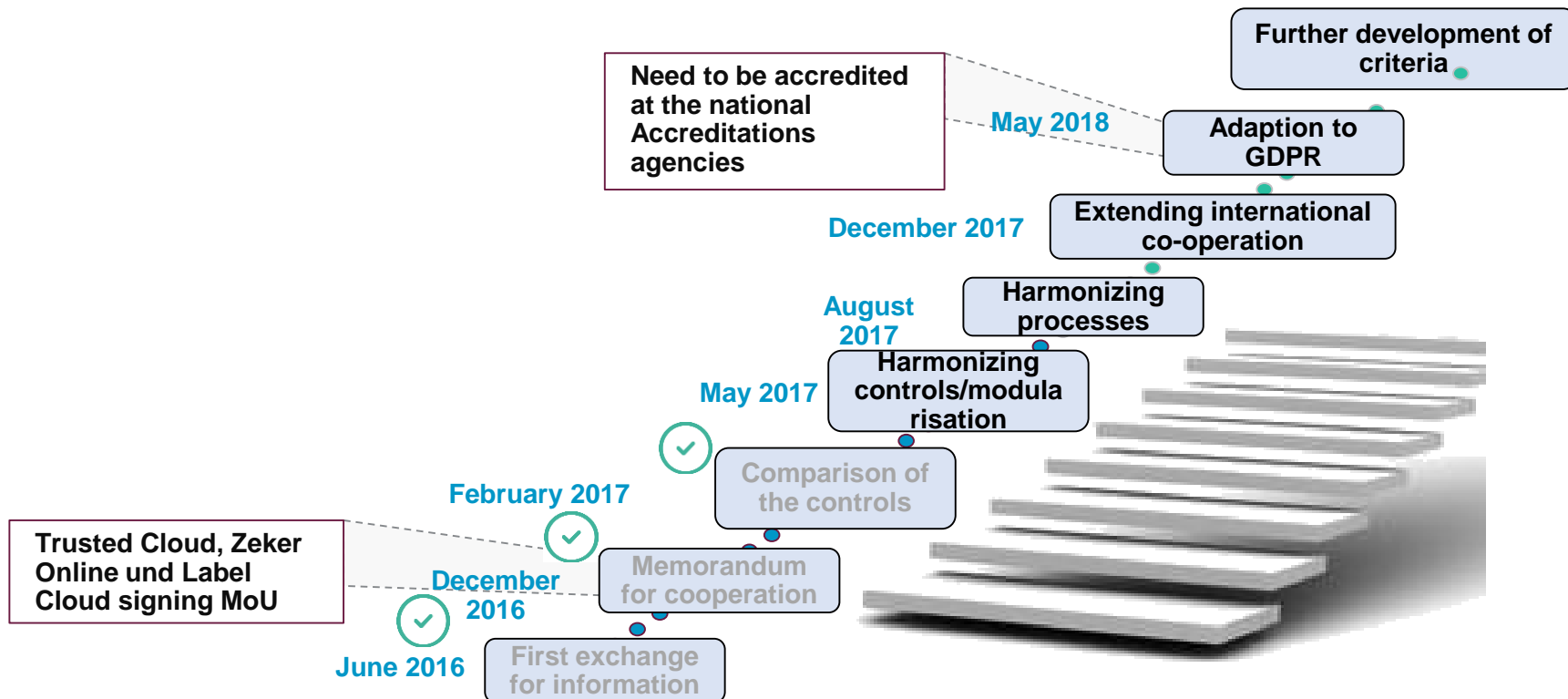Helping to **minimize** the **risk of exploitation**.

Building up **transparency** about cloud computing and cloud service

Professionalisation of cloud services (security, services etc.)

GDPR

- Article 42/43 - Certification
- …establishment of data protection **certification mechanisms** and of **data protection seals** and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors.
- The specific needs of **micro, small and medium-sized enterprises** shall be taken into account.

Roadmap

Further development of criteria

Need to be accredited at the national Accreditations agencies

May 2018

Adaption to GDPR

December 2017

Extending international co-operation

Harmonizing processes

August 2017

Harmonizing controls/modula risation

May 2017

Comparison of the controls

February 2017

Trusted Cloud, Zeker Online und Label Cloud signing MoU

Memorandum for cooperation

December 2016

June 2016

First exchange for information