EuroCloud

KC Class

Investing in your future
OPERATION PART FINANCED BY THE EUROPEAN UNION
European Regional Development Fund

Cloud Standardization, Compliance and Certification

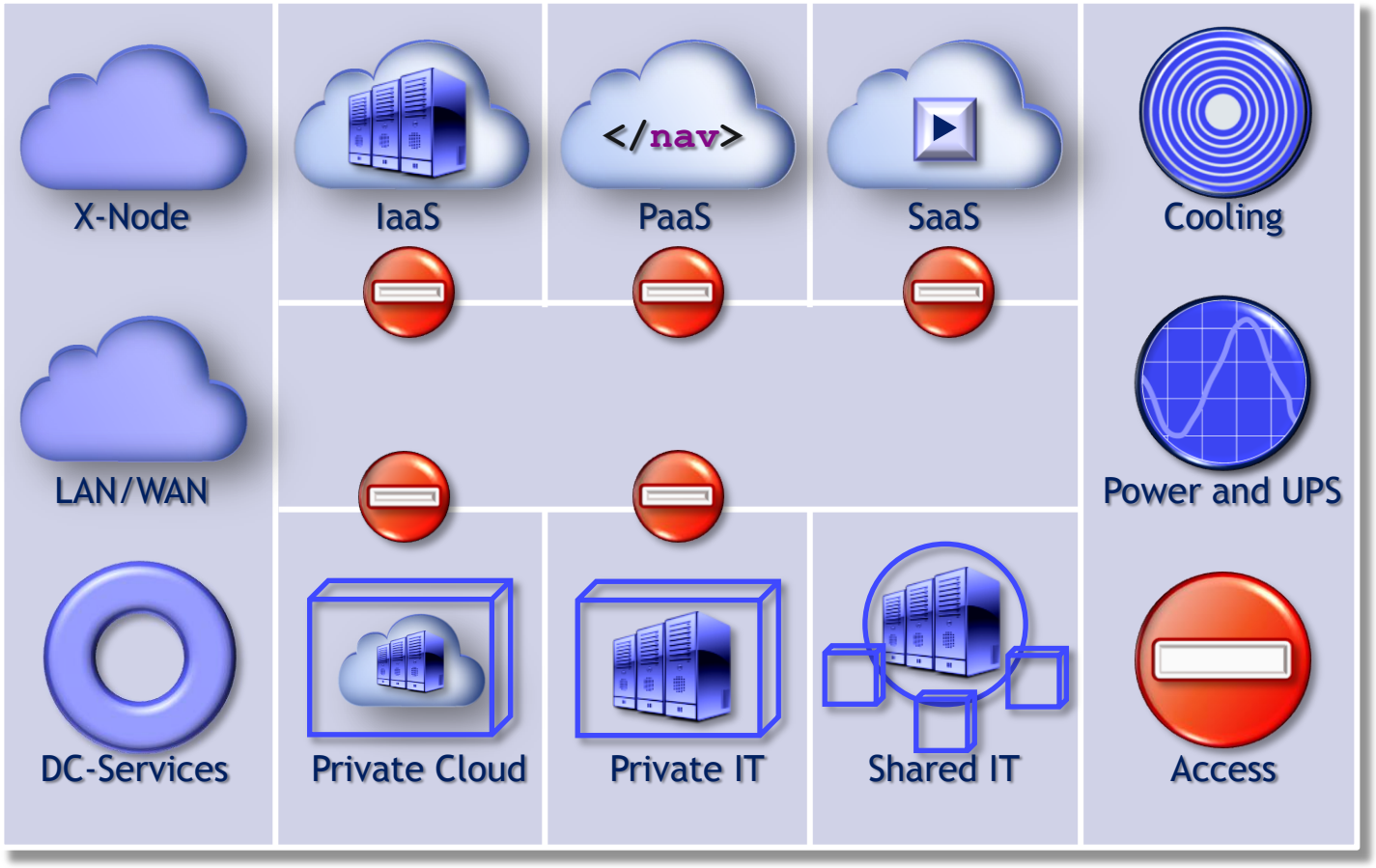
Class 2012 event

25.rd of October 2012
Dalibor Baskovc, CEO Zavod e-Oblak

Todays Agenda

- IT Resourcing with Cloud Computing and related challenges
- Landscape of standards and certification
- The role of Zavod e-Oblak within EuroCloud
- Conclusion

IT Resourcing - Data centric view



Datacenter risks

IT Provisioning

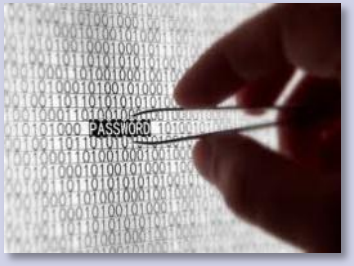
Cabling

Physical risks

Power supply

Cyber crime

Malicious insider



Unsecure devices

Cyberattack

Malware

What is important for Customers

Contract

Regulations

- Technical and legal security
- Legal compliance
- Availability and SLA compliance
- CSP reliability (including sub providers)
- Prevention of Lock In Situations
- Usability and sustainability
- …

Data Privacy

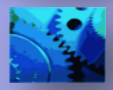
Data Security

Data Center and Location

Business Operations

Software, Interoperability

Cloud assessment requires a wide area for review

	Scope	Topics
	Contract	Terms and Conditions, SLA,…
	Regulations	Legal requirements, data location, data privacy directives, export control,..
	Data Security	ISMS, Access control, …
	Data Privacy	Data separation, data delition, access monitoring, …
	Data Center	Technical and mechanical environment
	Business Operations	Service Management
	Software Interoperability	Data export functionality and completness, general usability, transparency

IT Resourcing –Customer view

The European enterprise market

- Definition Small and Media Enterprises: up to 250 employees and less than 43 M sales per annum

	Number of enterprises	Persons employed	Value added	Apparent labour productivity
	(million)		(EUR 1 000 million)	(EUR 1 000 / person)
All enterprises	21.0	135.8	6 176	45.5
All SMEs	20.9	90.6	3 617	39.9
Micro	19.3	39.3	1 348	34.3
Small	1.4	27.9	1 147	41.2
Medium-sized	0.2	23.4	1 122	47.9
Large	0.0	45.2	2 559	56.6

http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-ET-11-001/EN/KS-ET-11-001-EN.PDF

Cloud Challenges

1	Efficiency of service provisioning
a	Usage of scalable architectures
c	Resource management & flexibility
d	Availability of services

2	Effectiveness of Services by users
a	Contracts incl. questions of liability
b	Control of Services by users
c	Governance/escalation mechanisms

3	Transparency of service delivery and billing
a	Billing incl. license management
b	Quality assurance and monitoring SLA
c	Type and location of Data processing

4	Information Security
a	Identity & rights management
b	Privacy & integrity
c	Access control, logging, attack prevention
d	Verification & certification

5	Data privacy

6	Interoperability
a	Migration in the/out of the Cloud
b	Ability to integrate into on-premise IT
c	Cloud federation

7	Portability between providers
a	Service portability
b	Data portability

8	Ensuring fair competition in the market

9	Compliance with regulatory requirements

Source Analyse by Booz & Company und FZI (2012)

Cloud specific risks

Data storage regional vs. global

Legal requirements

Lock in – data migration

Insufficient Interoperability

Shared environment

Mixed security requirements and data separation

Change of Roles System/Network/ Operating System

Hypervisor: CPU, Network, OS

Relevant standardization areas

	Type of standard	Examples
Technology	File & exchange format	OVF, EC2, USDL, CIM SVM,EDI…
	Programming models	MapReduce, JAQL; PIG, HIVE
	Protocols & Interface	OCCI. CDMI, Cloud Audit, Google DLF, ...
	Standard Components & reference architectures	OpenStack, OSGI, NIST RM, IBM RM, DMTF, CTP, ...
	Benchmark & tests	Benchmarking Suits, Security Assessment, ...
Management	Business models	IaaS, PaaS, SaaS operating models, Hybrid, Community
	Service Level Agreements	WS-Agreement (W3C), Business SLAs, ...
	Condition of contracts	EVB-IT, EU SVK, components of T&C, EULA
	Management models & processes	ISO 27001/27002, ITIL, COBIT, ...
	Controlling models & processes	SSAE, SAS 70, ...
	Guidelines	German BSI requirements, NIST UC, EuroCloud LDP&C
Legal	Legal requirements	EU data protection directive, national directive, Safe Harbor
	Voluntary Commitments	Open Cloud Manifesto, ...
	Company polices	Internal polices, ...

Source Analyse by Booz & Company und FZI (2012) - http://www.trusted-cloud.de/documents/BMWi_Cloud_Standards_Studie_e_web.pdf

Well known certification standards

ISO/IEC 27001 specifies requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a **management system -** an overall management and control framework - for managing an organization's information security risks. It does *not* mandate specific information security controls but stops at the level of the management system.

The standard ISAE 3402 and SSAE 16 require that management of the service organization provide a written assertion attesting to the fair presentation and design of controls (in a Type 1 report). This written assertion is separate from the written representation obtained from management.

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.

research, develop, publish and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals

Cloud specific auditing

EuroCloud works close together with national and international organizations in the area of Technology, Research, Public Administration, Security, Data Privacy and Legal topics. This joined competence has been used to prepare knowledge, specify quality criteria, support cloud service provider to achieve a differentiating quality level to be successful in a high competitive market and to show the maturity level of the services by gaining the EuroCloud Star Audit certification.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders.

Overview and Scope

Standard	General Scope	Areas addressed	Cloud Readyness	Comments
ISO 27001	Information Security Management System	Security, Compliance	Limited	Very generic. Need to understand which entity and what has been audited
COBIT	Information technology	IT Management	No	General Quality Framework
SAS 70/SSAE16/ ESAE3402	Transactions and Accounting	Book keeping compliance	Limited	Add on for ERP Cloud Services
EuroCloud Star Audit	Cloud Service (SaaS, PaaS, IaaS)	EU and national Law, Security, Compliance, EU and national Data Privacy, Interoperability	Yes	Common Scope, easy to understand for SMEs
FedRamp	Cloud Service Provider	Security, US Compliance, Continuous monitoring	Yes	Huge burocracy, partially self assessment Control against NIST SP 800-53 R3
CSA	Cloud Security	Security, Interoperability	Yes	Excellent security assessment
PCI DSS	CC Payment Services	Security	Limited	Very limited scope

Leading standardisation organisations in cloud computing

Europe	CC	**EuroCloud**	Comprehensive guidelines on law, data privacy and compliance, EuroCloud Star Audit (“Cloud Service quality mark”)
	ITC	**ETSI (European Telecommunications Standard Institute**	Standards, analysis of gaps and testing systems for interoperability, specifications, use cases, co-ordination, standardization roadmap
	ITC	**ENISIA (European Network and Information Security Agency)**	Cloud Computing – SME Survey, Cloud Computing Information Assurance Framework, Cloud Computing Risk Assessment

Source Analyse by Booz & Company und FZI (2012)

Resources to build Star Audit control sets

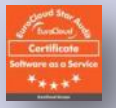
EuroCloud Competence

EuroCloud Star Audit

EuroCloud Self Assessment

EuroCloud SLA critieria catalog

EuroCloud Guidelines

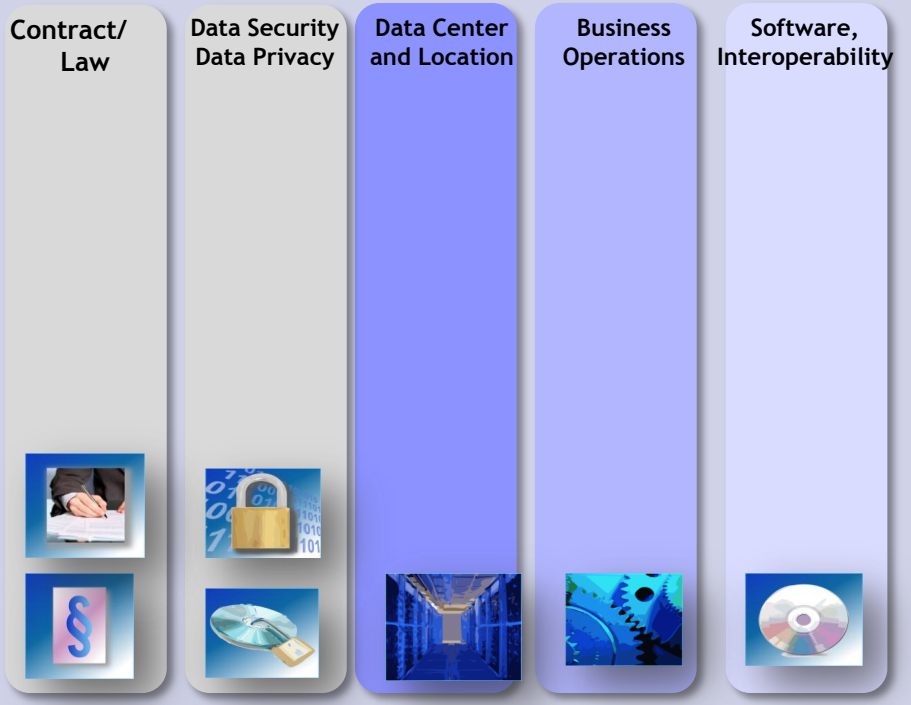


EuroCloud
CLOUD QUALITY INFORMATION PYRAMID

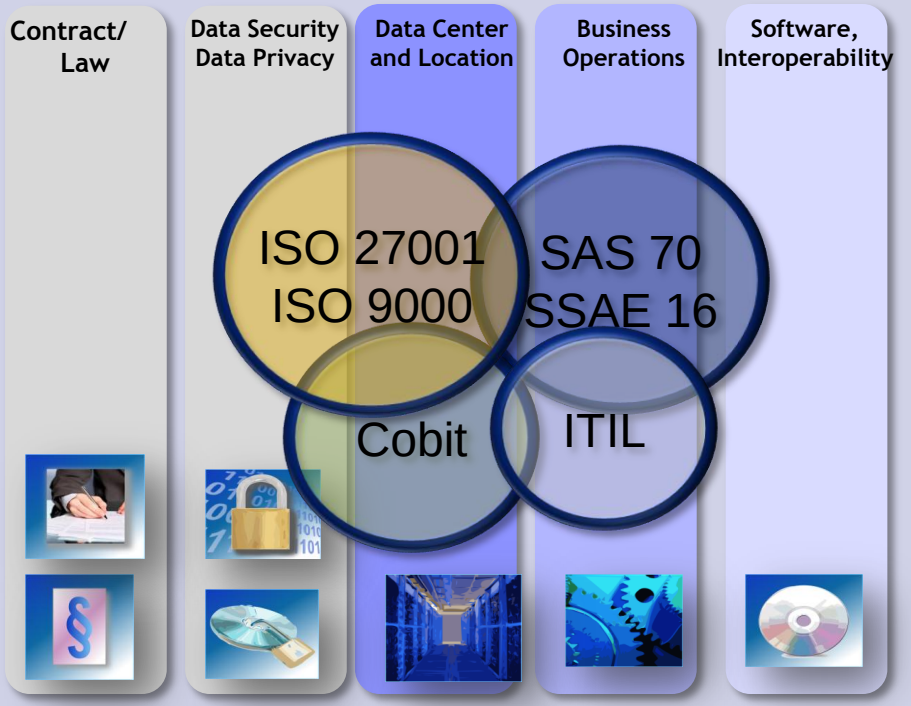
EuroCloud Star Audit has a common scope

- Statement about the reliability of the Cloud service, the service provider and involved sub-providers
- Examination of the specific contractual elements with view on
  - commissioned data processing
  - Data Protection Regulations
  - Book Keeping Regulations
- Operational processes
- SLA compliance
- Lock In situations and vendor change options
- Training and support
- Interoperability

EuroCloud Star Audit is the only cross over certification with common scope

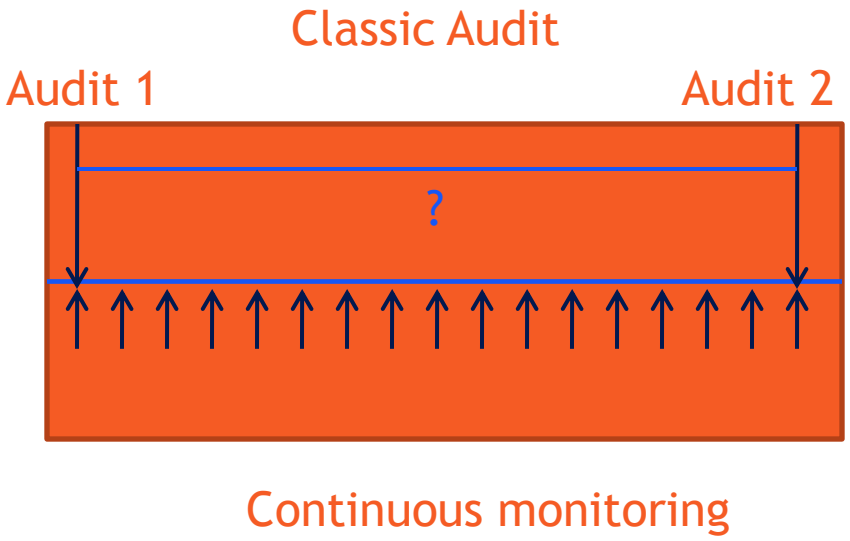


EuroCloud Star Audit is the only cross over certification with common scope



EuroCloud Star Audit is the only cross over certification with common scope

Future goal is continious monitoring



Conclusion

- Security, interoperability and legal compliance are success factors for a wide cloud adoption in Europe
- Cloud Services assessment is challenging, especially for SMEs
- Transparency about the CS supply chain is required
- The statement behind a certification should always be the same in order to be comparable
- We need standardization, legal harmonisation and ongoing knowledge transfer into the market

Futher links

- General Audit information
  - http://www.saas-audit.de/en/
- Study of the German Ministry of Economics and Technolgy
  - http://www.bmwi.de/English/Navigation/Service/publications,did=476736.html
- Guideline Law, Data Privacy and Compliance
  - http://en.eurocloud.de/2011/03/04/eurocloud-guidelines-cloud-computing-german-law-data-protection-and-compliance/
  - http://eurocloud.si/wp-content/uploads/EuroCloud-smernice-prevedeno-in-prilagojeno.pdf
- Slovene Cloud Computing and personal data protection guidelines from slovene data commisioner office and partners
- http://eurocloud.si/wp-content/uploads/Cloud-computing-and-data-protection-ENG-final1.pdf
- Webinar Cloud Security
  - http://en.eurocloud.de/2010/09/01/09-09-10-webinar-cloud-security/

Thank you for your attention!
Any Questions - if not further details
dalibor.baskovc@eurocloud.si