

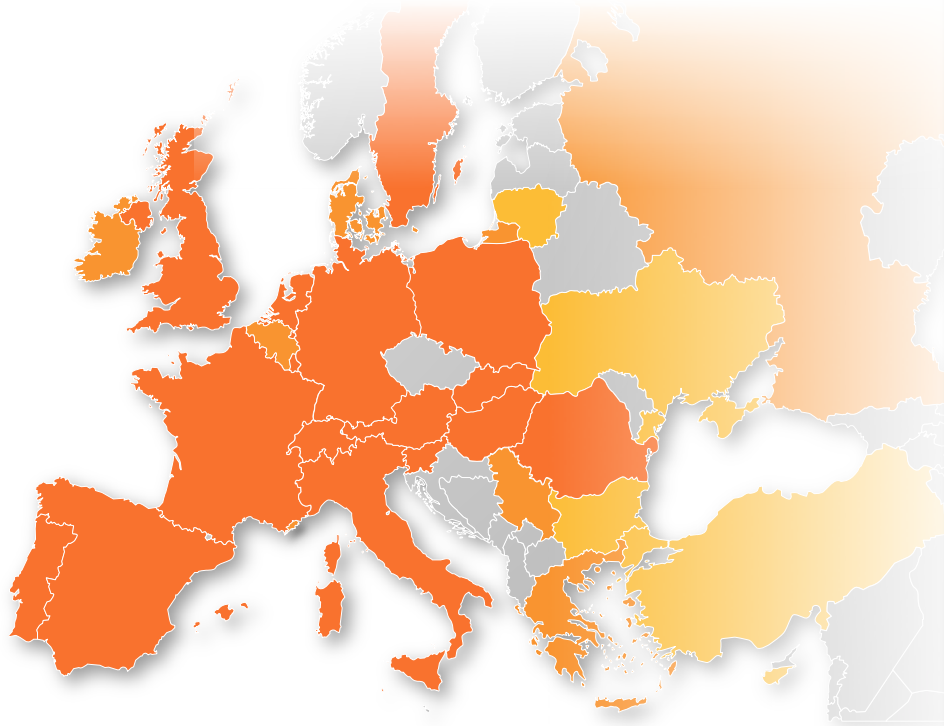
EuroCloud Deutschland_eco e.V

eco KG Sicherheit – 25.02.2015

Cloud Security und Monitoring von kritischen Parametern

Andreas Weiss – EuroCloud Deutschland_eco e.V.

Über das EuroCloud Netzwerk



- 22 Länder
- +10 Kandidaten
- Netzwerk von > 300 Cloud Spezialisten
- > 1000 Mitgliedsunternehmen in den Ländern
- Arbeitsbereiche
 - Customers Confidence in Cloud
 - Standards and Interoperability
 - Legal Framework Harmonization
 - Linking Europe's Cloud Industry globally
 - Research and Innovation
 - Start-Up Encouragement

Internationale Vernetzung



- Gemeinsame Initiativen und Projekte
- Konferenzen
- Awards
- ECSA - Zertifizierung



- Digital Agenda
- Cloud Select Industry Group
 - SLA
 - Code of Conduct
 - Certification



- Cloud Certification
- Cloud Risk assessments
- Cloud Security Guide fo SMEs
- Cloud Resilience



- Cloud Standards
- Interoperability
- SLA

Basisthemen

- Recht und Compliance
- Service Level Agreements
- Security
- Datenschutz

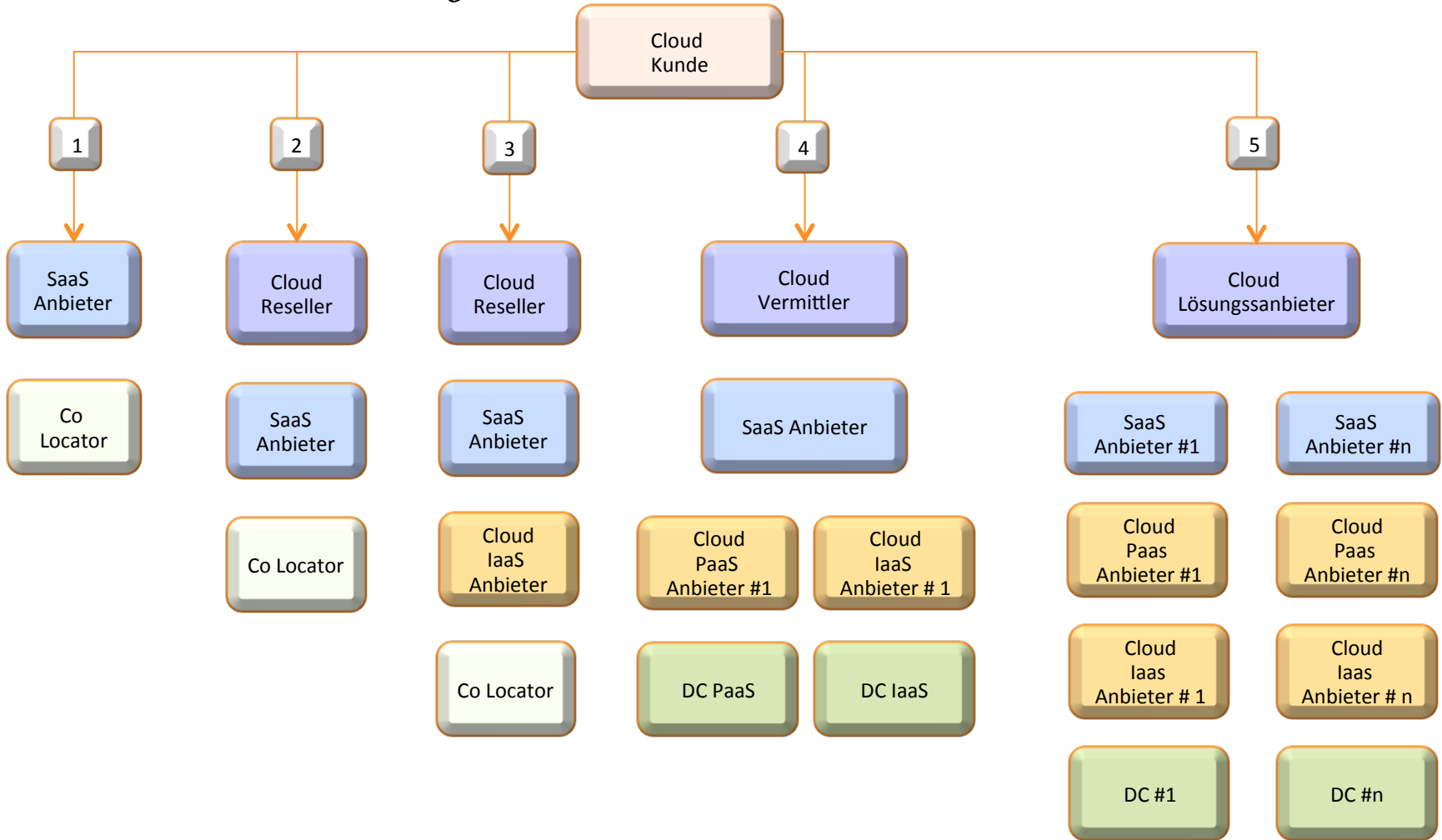
www.eurocloud-staraudit.eu

www.ngcert.eu

Die Herausforderung

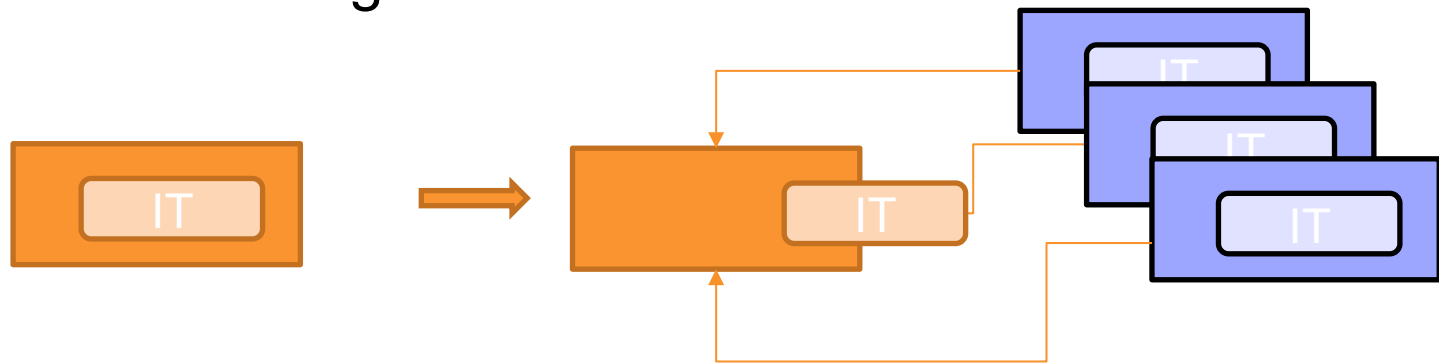
- Cloud Services sind als **Lieferkette** zu betrachten und besitzen eine hohe Agilität im technischen Aufbau
- Kein Cloud Service **gleich** dem anderen
- Perimeterschutz ist nur noch ein **untergeordnetes** Schutzelement
- Technische Systeme müssen permanent gegen Angriffe von **außen und von innen** überwacht werden
- Fragen zur technischen und organisatorischen Sicherheit, zum **Datenschutz** und zur Servicequalität stehen an **oberster** Stelle

Cloud Zuliefererkette



IT Abteilung als Broker

- Die IT Abteilungen der Unternehmen müssen sich zunehmend um IT Services kümmern, deren Betriebsverantwortung bei externen Anbietern liegt.



<http://www.enisa.europa.eu/media/press-releases/new-enisa-report--the-double-edged-sword-of-cloud-computing-in-critical-information-infrastructure-protection>

ENISA – C-SIG Certification

■ CCSL - Cloud Certification Schemes List

Welcome to the Cloud Certification Schemes List (CCSL) - a list of different certification schemes which could be relevant for potential cloud computing customers. The creation of this list is explicitly mentioned as a key action in the European Cloud Strategy. This list was developed by ENISA in tight collaboration with the European Commission and the private sector (see below).

What is a cloud certification scheme?

Before buying a cloud service, customers want to know if the service is secure and reliable. But cloud computing services are complex and built up from many different IT components (servers, large data centres, software, etc. indeed), and so hard for individual customers to check all the technical details by themselves. Cloud providers have many customers. One of the main uses of cloud computing is if all customers would check their security requirements separately, then this would make double work. If each customer would want to do an on-site audit, for example, there would be long queues at the gates of data centres. Now, the idea of a certification scheme is to check one level of security requirements, once for all customers. In this way, certification can simplify the procurement of cloud services for customers. Most cloud certification schemes do not require the need for customers to do on-site audits before procuring a certification, one way to simplify the process.

We refer the interested reader to a paper ENISA published last year which gives an overview of a range of information security certification schemes, used in different sectors.

How to use this list?

CCSL gives an overview of different existing certification schemes which could be relevant for cloud computing customers. CCSL also shows which are the main characteristics of each certification scheme. For example, CCSL schemes are ranked by "which are the underlying standards?", "who issues the certification?", "is the cloud service provider audited?", "who audits?", etc. often, CCSL provides links and references to each certification schemes for further reading.

Cloud Certification schemes

Click on the icons of each certification scheme below, to view the characteristics of each scheme. In the future more certification schemes will be listed. The icons are shown in random order.

Background of this work

In 2012 the EC issued a communication titled "European Strategy for Cloud Computing - unlocking the potential of cloud computing in Europe". One of the actions outlined there is to speed the procurement of IT via vendor certification schemes and a list of such schemes. In the strategy ENISA is asked to support this work. Taking up this, ENISA developed this list, in tight collaboration with the European Commission and the private industry. (Cloud Certification and C-SIG). The creation of this list is explicitly mentioned as a key action in the European Cloud Strategy. Read more about the background of the work in ENISA's paper on Certification in the EC Cloud Strategy.

Why these schemes are listed and not others?

The selected industry Cloud certification schemes are high-level principles and also a preliminary list of certification schemes (see page 7 of ENISA's paper on Certification in the EC Cloud Strategy). We started with a subset of this list and asked the relevant organisations to fill in information about their certification schemes.

Something missing or want to contribute to this work?

If you would like to suggest another certification scheme to be added to this list, or if you would like to join this work and help improve this list, please send a message to Cloud.Security@enisa.europa.eu.

Feedback or comments?

If you would like to give us feedback or comments on this list of schemes, or about a specific scheme on the list, please send a message to Cloud.Security@enisa.europa.eu.

For members of the C-SIG on Certification

To access the CCSL list, for meeting charges, and proposing new schemes, navigate here.

The email on this list is found here.

If you want to make comments or request changes to the listing please use the issue tracker.

If you have problems logging in, or if you forgot your password please send a message to Cloud.Security@enisa.europa.eu.

Ziele:

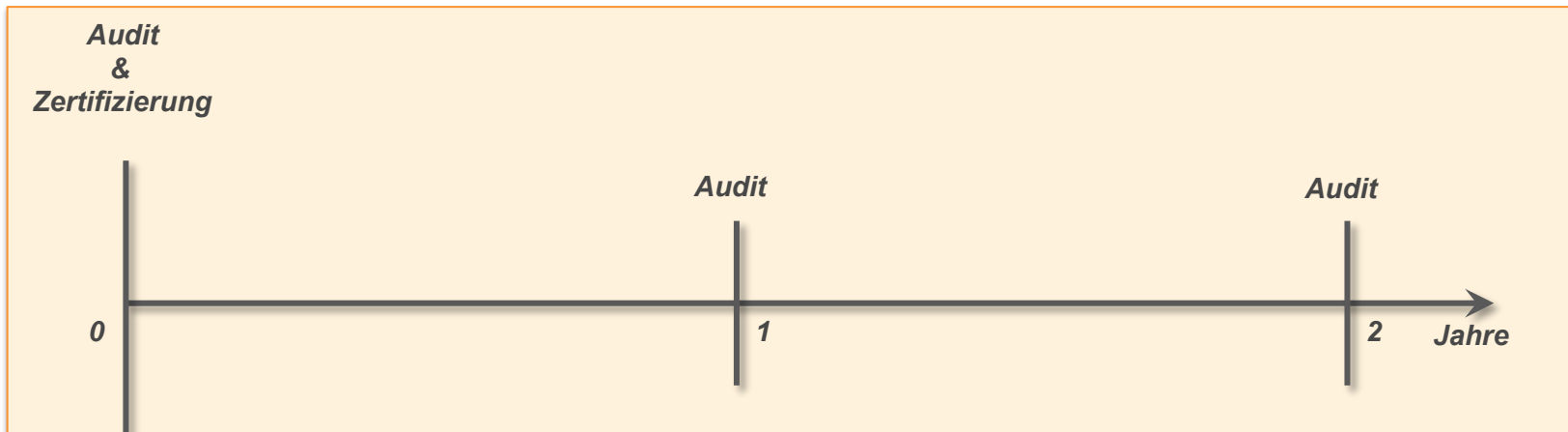
- *Transparenz zu diversen Zertifizierungen*
- *Darstellung der organisatorischen Hintergründe*
- *Differenzierung nach Audit und Selbstaussage*

<https://resilience.enisa.europa.eu/cloud-computing-certification>

Traditionelle Zertifizierungsansätze



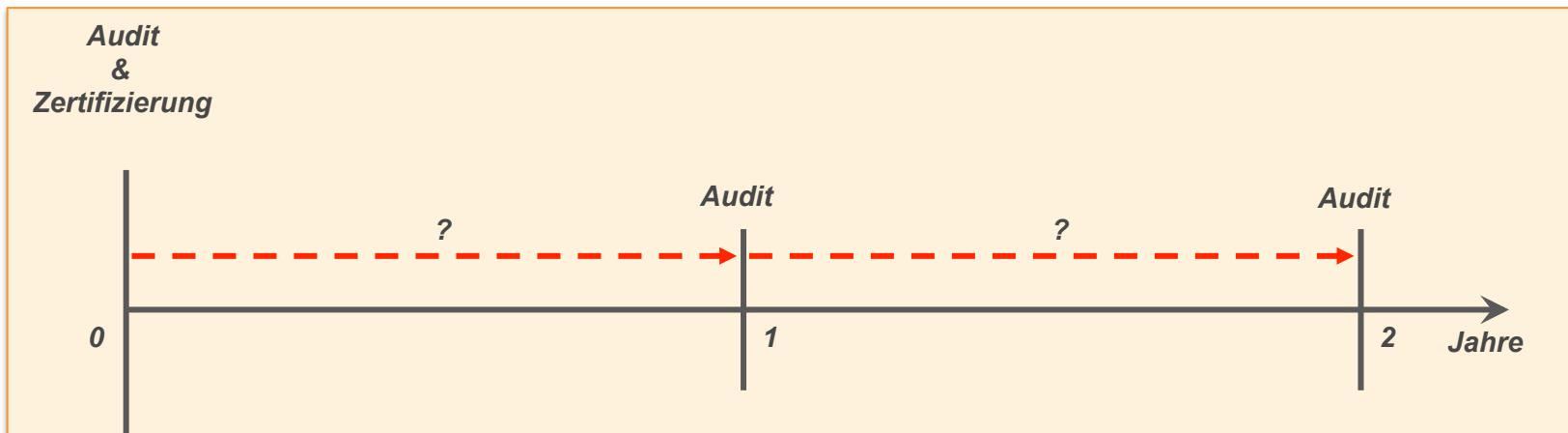
- Manuelle Prüfung von Anforderungen eines Zertifikates
- Statische Prüfungsintervalle (bzw. Gültigkeit) von ein bis drei Jahren



Problem traditioneller Zertifizierungsansätze



- Zwischen den Prüfungspunkten verändert sich der zertifizierte Cloud-Service
- Die Nicht-Erfüllung von Anforderungen eines Zertifikates kann eintreten, ohne bemerkt zu werden

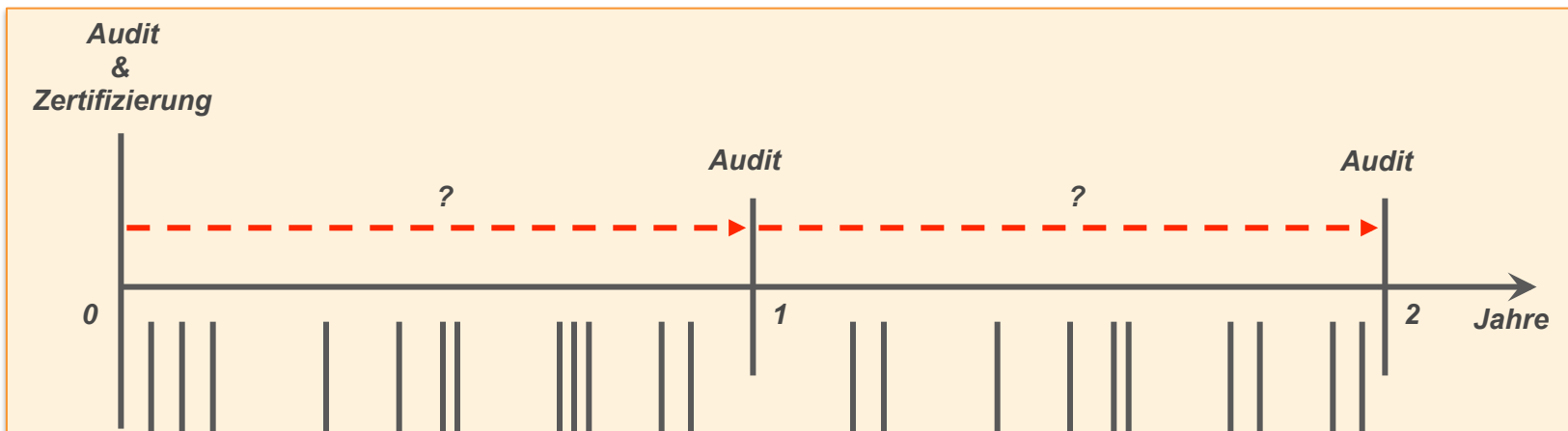


Lösung:

Automatisierte und fortlaufende Prüfung der Anforderungen



- Automatisierter Abgleich von High-Level Anforderungen eines Zertifikates mit Informationen über den Cloud-Services (z.B. Verhalten anhand von Monitoringdaten zur Laufzeit des Services)



Dynamische Zertifizierung



Cloud Computing

- Hohe Dynamik und rasanter technischer Fortschritt bei Cloud-Services
- Hohe Anforderungen deutscher Unternehmen hinsichtlich Qualität, Datenschutz und Datensicherheit von Cloud-Services
- Hohe Komplexität durch Rekombination von Cloud-Services

Zertifizierungen

- Viele Zertifikate existierten bereits vor der Cloud-Ära; jedoch wenige spezialisierte Zertifikate
- Bestehende Zertifikate stellen eine Momentaufnahme dar; Gültigkeit von 1-3 Jahren
- Werden die Auditkriterien nach Konfigurationsanpassungen noch eingehalten?

Forderung: *Kontinuierlicher Nachweis des Zertifizierungsstatus mit Hilfe einer dynamischen Zertifizierung*

Dynamische Zertifizierung

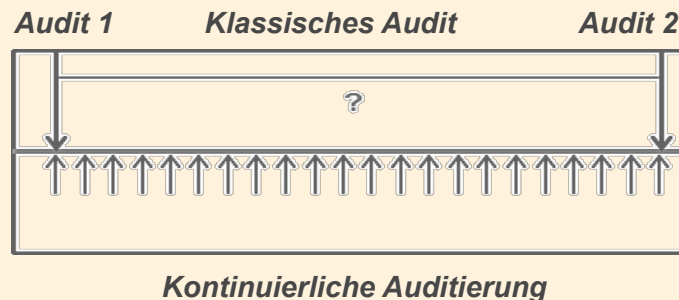


Entwicklung von Verfahren zur (teil-) automatisierten Analyse von cloud-basierten Prozessen auf die Einhaltung kritischer Anforderungen z.B.:

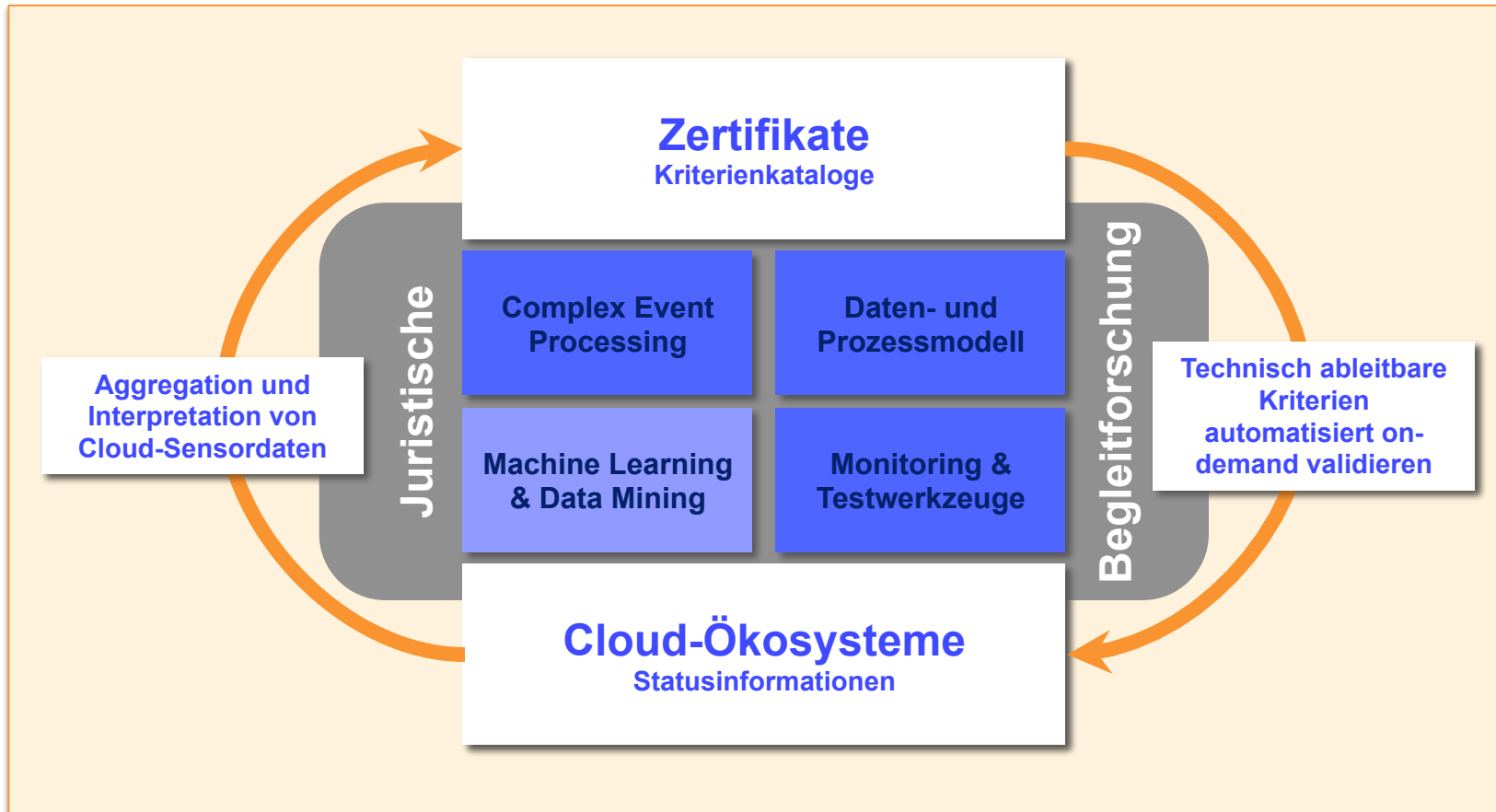
- Sicherheit
- Verfügbarkeit
- Datenschutz
- Servicevereinbarungen
- Geschäftsbedingungen

Das bedeutet:

- Kontinuierliche Auditierung von Cloud-Services auf Basis von definierten Kennzahlen
- Automatisierung von Elementen des Prüfprozesses
- Technische, organisatorische, rechtliche und wirtschaftliche Rahmenbedingungen für die Integration in den Regelbetrieb des Anbieters



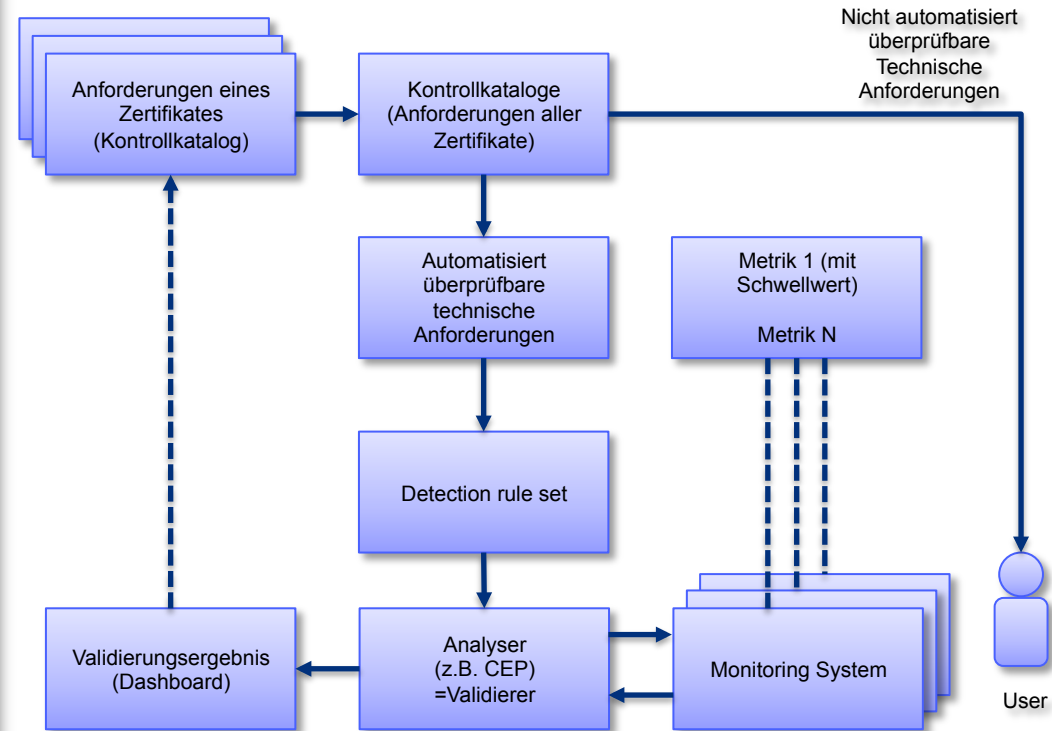
Im Detail



Dynamische Zertifizierung von Cloud-Infrastrukturen

Hypothesen:

- Es ist möglich, kritische Anforderungen eines Zertifikats automatisiert zu prüfen.
- Eine rein automatisierte Zertifizierung ist (nur) für einzelne Prüfschritte möglich.
- Mit Hilfe automatisierter Prüfschritte kann die Erfüllung von Anforderungen hinsichtlich Qualität, Datenschutz und Datensicherheit rechtssicher erbracht werden.



Voraussetzungen



- **Spezifikation der Anforderungen** *in Form von Anwendungsfällen für eine dynamische Zertifizierung, sowie Beschreibung eines Referenzmodells;*
- **Definition eines Kennzahlensystems** *inklusive der (teil-)automatisierten Mess- und Vergleichsverfahren sowie eine Taxonomie zur Beschreibung von Cloud-Services als Grundlage für eine dynamische Zertifizierung;*
- **Design der Systemarchitektur und des Vorgehens für das kontinuierliche Monitoring** *sowie Reporting an die unterschiedlichen Interessengruppen;*
- *Dokumentation möglicher* **Vertragsrahmen, der organisatorischen und betrieblichen Aspekte, der wirtschaftlichen Betrachtung sowie der Akzeptanz;**
- **Prototypische Implementierung** *von Basis-Komponenten, von Monitoring-Services sowie eines (teil-)automatisierten Zertifizierungsdienstes*
- **Evaluationsergebnisse und Erprobungsbericht** *aus den Pilotierungen bei den Feldpartnern*
- **Wissenschaftliche Publikationen**

Neues Sicherheitsdenken

- Es gibt keine allgemeine Cloud Sicherheit, jede Serviceverbindung muss für sich betrachtet werden.
- Der Begriff Sicherheit in der Cloud Ära sollte neu definiert werden.
- Durch kontinuierliche Prüfung kritischer Faktoren in allen genutzten Diensten kann ein für dritte nachvollziehbares angemessenes Schutzniveau erreicht werden

ECSA Katalog und Self Assessment

<https://eurocloud-staraudit.eu/home/publications/ecsa-controls.html>

<https://assessment.eurocloud-staraudit.eu/>

No.	Control Statement	Control Scope	Control Question	Star Rating	Asset Goal	Submissions
A02-501-C01-Q01	Appropriate Customer Support	Validation of Support Service	How is user authentication undertaken with regard to support?	**** (A) **** (B)	A - Secret token by Phone, two factor authentication online	

1 Adequate contract terms

1.1 Conclusion of contract

1.1.1 A02-501-C01-Q01

Control:	Are the contract elements accessible for the customer before booking services?
Rating:	***
Goal:	Online reference or request procedure for clients
Submissions:	Please provide online reference or contract bundle
Status:	Mandatory

Score	Assessment	Target
A	Excellent	All relevant contract elements are bundled, easy to understand, easily accessible on the website with the most recent version and version management. No hidden links to any other documents that have legal binding.
B	Good	All relevant contract elements are available online with version management. No hidden links to any other documents that are legally binding.
C	Sufficient	All relevant contract elements are available upon request. Links to other contracts are existing and contract layout is according to market standards.
D	Major gaps	Not all elements of the contract are available in actual versions.
E	Not acceptable	Some of the contract elements are missing or are not compliant with legal regulations.
F	Not applicable	Internal contractual relationship or internal assessment of service.

Reference Information:

SLA EU Document:
Contract elements: A contract may consist of the following elements:
File contract information:
http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_pci_en.pdf

Unfair contract terms:
http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_unfair_contract_terms_en.pdf

Date: 22/09/14
Version 3.0 Rev 4

EuroCloud Europe a.s.3.
EuroCloud Star Audit Audit Scope

HOME SAVE CLEAR PRINT PREVIOUS NEXT

02 Contract & Compliance

0% 100%

Scope: Adequate contract terms

Control: Conclusion of contract

★★★★★

A02-501-C01-Q01 - Are the contract elements accessible for the customer before booking services?

Goal: Online reference or request procedure for clients

Choose one of the following answers

- A: Excellent - All relevant contract elements are bundled, easy to understand, easily accessible on the website with the most recent version and version management. No hidden links to any other documents that are legally binding.
- B: Good - All relevant contract elements are available online with version management. No hidden links to any other documents that are legally binding.
- C: Sufficient - All relevant contract elements are available upon request. Links to other contracts are existing and contract layout is according to market standards.
- D: Major gaps - Not all elements of the contract are available in actual versions.
- E: Not acceptable - Some of the contract elements are missing or are not compliant with legal regulations.
- F: Not applicable - Internal contractual relationship or internal assessment of service.
- G: No answer

Reference

Please provide online reference or contract bundle

Comment:

Consider to reshape the Goal description to be more in sync with typical ISO 27001 control description

What is the gap to achieve a certification extension for

a) EU
b) Germany

for an already certified service.

Reference Information:

SLA EU Document

Contract elements: A contract may consist of the following elements:

File contract information
http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_pci_en.pdf

Unfair contract terms:
http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_unfair_contract_terms_en.pdf

Previous Next

Danke für Ihre Aufmerksamkeit!



Andreas Weiss

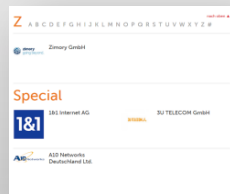
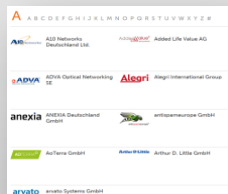
Direktor EuroCloud Deutschland_eco e.V.
andreas.weiss@eurocloud.de

- www.eurocloud.de
- www.ecd-conference.de
- www.eurocloud.org
- www.cloudingsmes.eu
- www.cloud-migration.eu
- www.eurocloud-staraudit.eu
- www.cloudcatalyst.eu
- www.trustincloud.org
- www.eurocloudcongress.org

Mitglieder EuroCloud und gemeinsame Aktivitäten

- Derzeit 135 Mitglieder
- Struktur
 - Cloud Service Anbieter
 - DC Betreiber
 - ISP, Hosting & Managed Services
 - Berater
 - WP und Recht
 - Systemhäuser

<http://www.eurocloud.de/ueberuns/mitgliederliste.html>



- Leitfäden (KG)
 - Erläuterung der Rahmenbedingungen
 - Verständliche Terminologie
 - Empfehlungen und Checklisten
- Events
 - Kongresse
 - Messen
 - Roadshows
 - Firmenevents
- Pressearbeit
 - Award und Best Practice
 - Rechtsfragen
 - Datenschutz
 - Datensicherheit
- Initiative und Netzwerke
 - EuroCloud Europe
 - Trusted Cloud
 - EU Projekte

Initiativen und Förderprojekte

- CloudingSMEs
- Cloud Catalyst
- Trusted Cloud
- NGCert
- Horizon 2020
- Trust in Cloud (AT)



EuroCloud-Projekte: Engagement auf europäischer Ebene

EuroCloud ist in eine Reihe von europäischen Projekten eingebunden, die von der EU-Kommission gefördert werden.

Projekt CloudingSMEs

Das Projekt wurde Mitte 2013 mit einem Konsortium von Anwender- und Anbieterverbänden, technischen Integratoren und unter Mitwirkung der Messe Karlsruhe gestartet. Es richtet sich an KMU und bietet umfangreiche Hilfe bei dem Aufbau von Wissen, der Planung und Integration von Cloud-Diensten.

www.cloudingsmes.eu



Projekt Cloud Catalyst

Das Projekt ist besonders auf Start-up-Unternehmen für den Aufbau innovativer Cloud Services aus Europa ausgerichtet. Auch hier werden die Bedürfnisse von KMU bei der Nutzung berücksichtigt.

www.cloudcatalyst.eu