SEcure Cloud computing
for CRitical Infrastructure IT

High Assurance in Multi-Layer Cloud Infrastructures

PhD Research Agenda[1]

Austrian Institute of Technology (AIT) / Technical Univsersity of Vienna
Aleksandar Hudic

[1] Hudic A., Mauthe A., Caceres S., Hecht T., Tauber M. : "Towards continuous Cloud Service Assurance for Critical Infrastructure IT", IEEE FiCloud-2014

AIT Austrian Institute of Technology • ETRA Investigación y Desarrollo • Fraunhofer Institute for Experimental Software Engineering IESE • Karlsruhe Institute of Technology • NEC Europe • Lancaster University • Mirasys • Hellenic Telecommunications Organization OTE• Ayuntamiento de Valencia • Amaris

Research questions

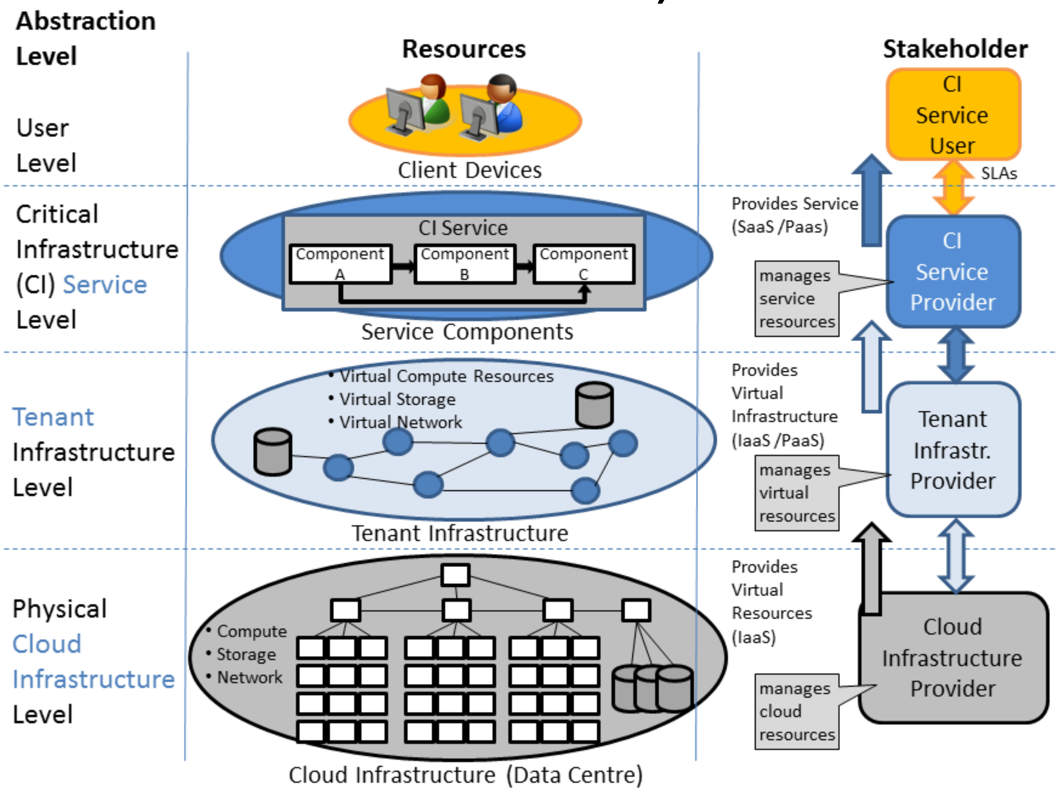
How to assure that security properties are met across distinct cloud layers with different stake holders?

How to derive continuous assessment of security properties across the clouds architecture?

How can security be assessed, measured or scaled in respect to a certain predefined set of security properties (assurance levels)?

How to aggregate/inherit security across different stake holders in Cloud?

Levels of Abstraction (The SECCRIT architecture)



Abstraction Level | Resources | Stakeholder

User Level — Client Devices — CI Service User (SLAs)

Critical Infrastructure (CI) Service Level — CI Service: Component A, Component B, Component C — Service Components — Provides Service (SaaS /Paas) — manages service resources — CI Service Provider

Tenant Infrastructure Level — • Virtual Compute Resources • Virtual Storage • Virtual Network — Tenant Infrastructure — Provides Virtual Infrastructure (IaaS /PaaS) — manages virtual resources — Tenant Infrastr. Provider

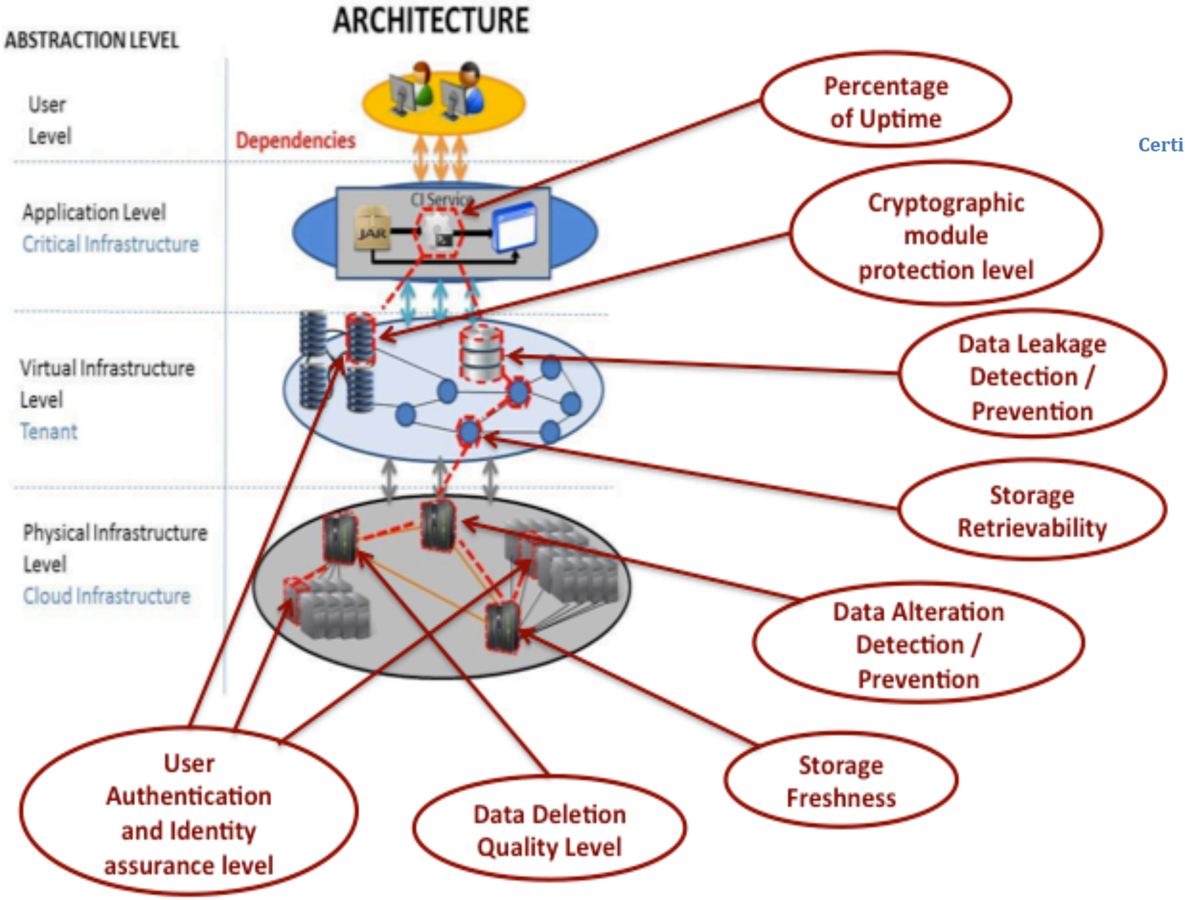
Physical Cloud Infrastructure Level — • Compute • Storage • Network — Cloud Infrastructure (Data Centre) — Provides Virtual Resources (IaaS) — manages cloud resources — Cloud Infrastructure Provider

R. Bless, Flittner, M., Horneber, J., Hutchison, D., Jung, C., Pallas, F., Schöller, M., Shirazi, S. Noor ul Ha, Simpson, S., and Smith, P., “Whitepaper "AF 1.0" SECCRIT Architectural Framework”. 2014. (and IEEE CloudCom)

Research Activities

- Establish a catalogue of the most relevant security concerns (based on established work)
  - Classify them per classes
  - Distinguish their relevance
- Provide a compact methodology for assessment and aggregation of these security concerns horizontally and vertically
- Define policy of aggregation for certain set security properties
- Propose an empirical evaluation of the methodologies proposed

Security properties


ARCHITECTURE
ABSTRACTION LEVEL
User Level
Dependencies
Application Level
Critical Infrastructure
CI Service
JAR
Virtual Infrastructure Level
Tenant
Physical Infrastructure Level
Cloud Infrastructure
Percentage of Uptime
Cryptographic module protection level
Data Leakage Detection / Prevention
Storage Retrievability
Data Alteration Detection / Prevention
Storage Freshness
Data Deletion Quality Level
User Authentication and Identity assurance level

Certification infrastrUcture for MUlti-Layer cloUd Services

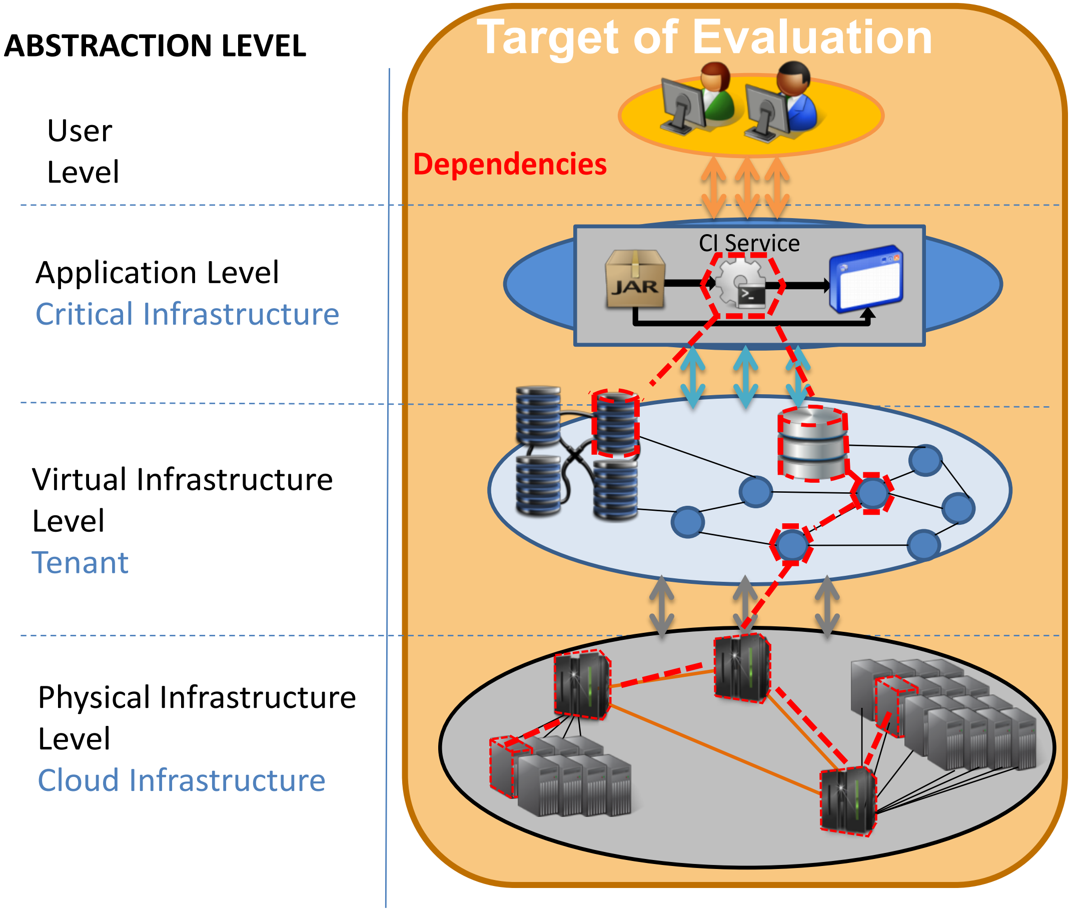
- Security-aware SLA specification language and cloud security dependency model
- Certification models
- Core Certification mechanisms

SEcure Cloud computing for CRitical infrastructure IT

- Methodologies for Risk Assessment and Management

- The Notorious Nine: Cloud Computing Top Threats in 2013

Assurance Assessment Framework



ABSTRACTION LEVEL

User Level

Application Level
Critical Infrastructure

Virtual Infrastructure Level
Tenant

Physical Infrastructure Level
Cloud Infrastructure

Framework elements:

- Component of Evaluation (CoE)
  - Component dependencies (CD)
  - Association (AS)
- Group of Evaluation (GoE)
- Target of Evaluation (ToE)

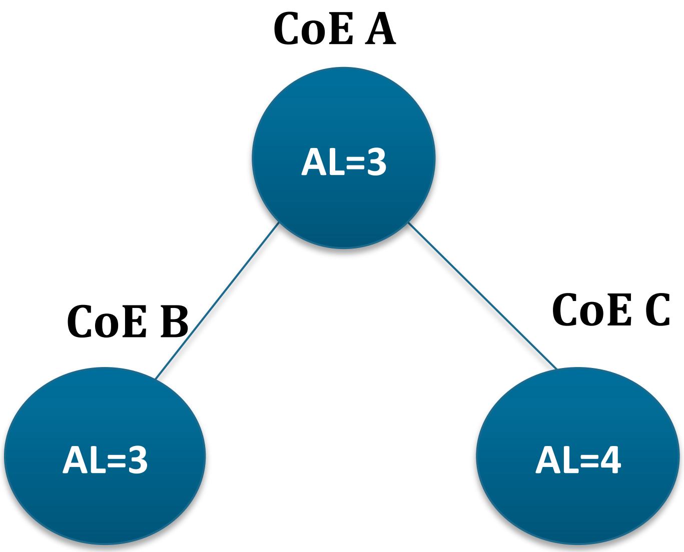
Assurance Profile:

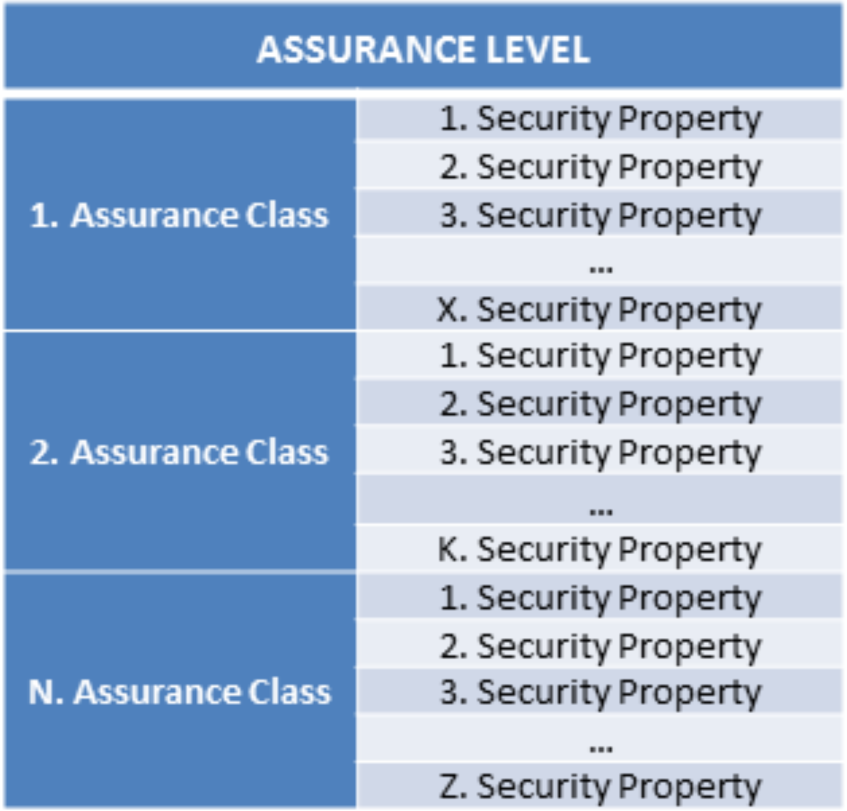
- Assurance Type (AT)
- Assurance Properties (AP)
- Assurance Class (AC)
- Security Objectives (SO)
- Assessment Interval (AI)

Common Criteria Framework for Information Technology Security Evaluation, CCDB USB Working Group, 2012, part 1-3. Online available: http://www.commoncriteriaportal.org.

Aggregation Policies (1)

Tree model:

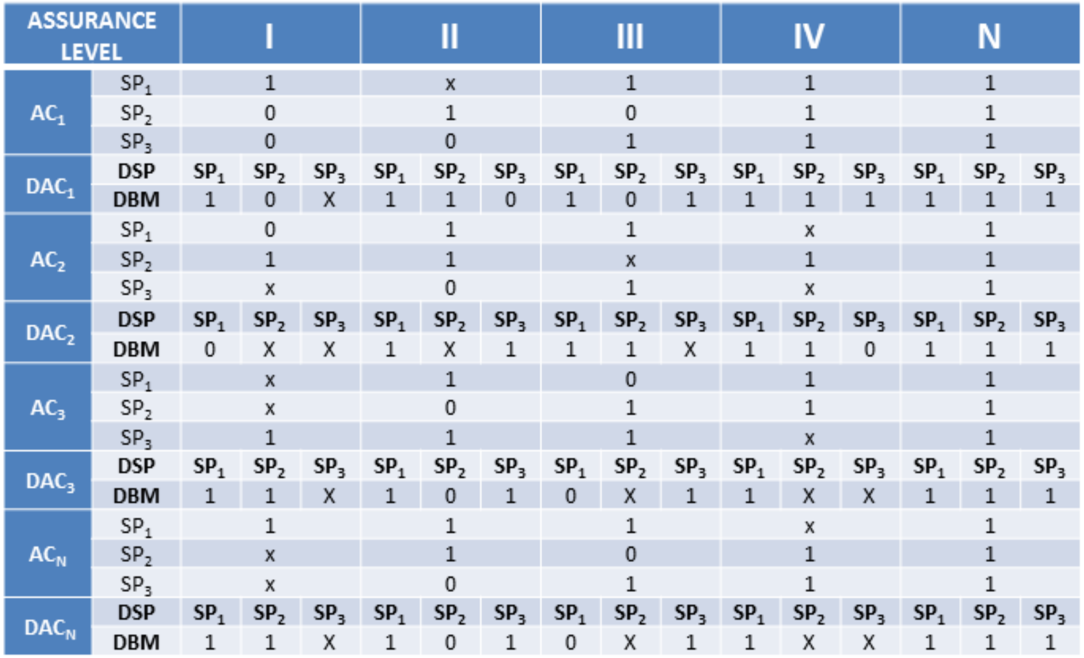




ASSURANCE LEVEL	
1. Assurance Class	1. Security Property
	2. Security Property
	3. Security Property
	...
	X. Security Property
2. Assurance Class	1. Security Property
	2. Security Property
	3. Security Property
	...
	K. Security Property
N. Assurance Class	1. Security Property
	2. Security Property
	3. Security Property
	...
	Z. Security Property

Aleksandar Hudic, Thomas Hecht, Markus Tauber, Andreas Mauthe, and Santiago Caceres Elvira, "**Towards Continuous Cloud Service Assurance for Critical Infrastructure IT**", IEEE International Conference on Future Internet of Things and Cloud (FiCloud 2014)

Aggregation Policies (2)



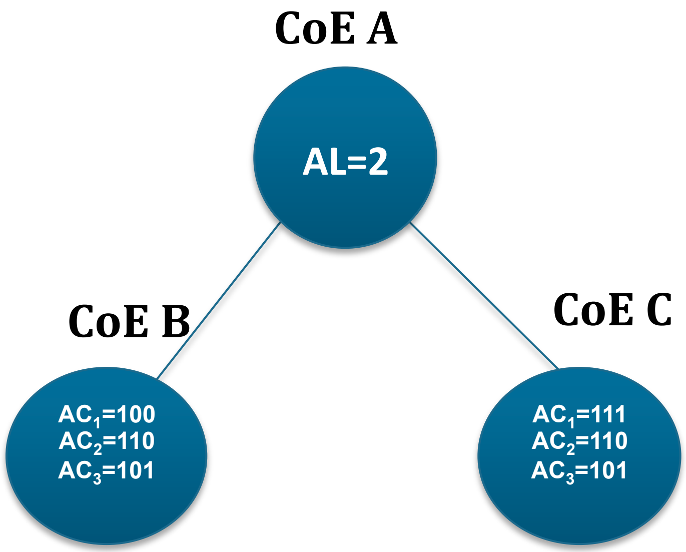
ASSURANCE LEVEL		I			II			III			IV			N		
AC_1	SP_1	1			x			1			1			1		
	SP_2	0			1			0			1			1		
	SP_3	0			0			1			1			1		
DAC_1	DSP	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3
	DBM	1	0	X	1	1	0	1	0	1	1	1	1	1	1	1
AC_2	SP_1	0			1			1			x			1		
	SP_2	1			1			x			1			1		
	SP_3	x			0			1			x			1		
DAC_2	DSP	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3
	DBM	0	X	X	1	X	1	1	1	X	1	1	0	1	1	1
AC_3	SP_1	x			1			0			1			1		
	SP_2	x			0			1			1			1		
	SP_3	1			1			1			x			1		
DAC_3	DSP	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3
	DBM	1	1	X	1	0	1	0	X	1	1	X	X	1	1	1
AC_N	SP_1	1			1			1			x			1		
	SP_2	x			1			0			1			1		
	SP_3	x			0			1			1			1		
DAC_N	DSP	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3	SP_1	SP_2	SP_3
	DBM	1	1	X	1	0	1	0	X	1	1	X	X	1	1	1

Policy Elements:

- Dependency Assurance Class (DAC) - defines the requirement for the underplaying objects in terms of security properties
- Dependency Security Properties (DSP) - defined set of properties for the underplaying objects
- Dependency Assurance Class (DBM) – bitmask which defines minimum requirements per Security Property for underplaying objects

Aggregation Policies (3)

Tree model:



Features:

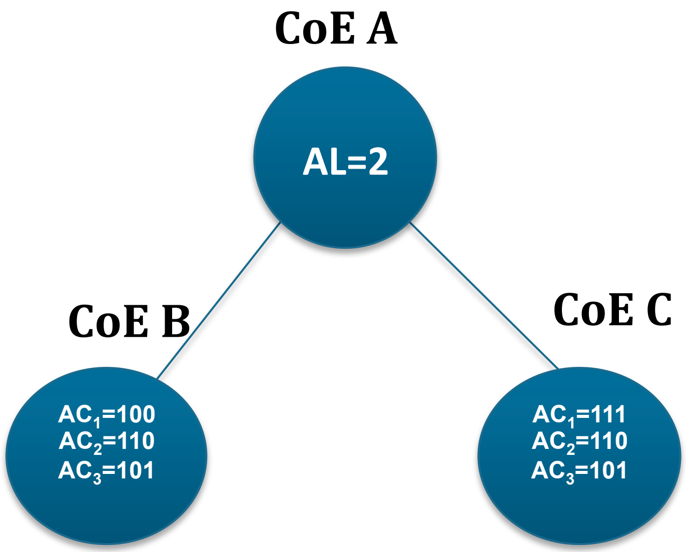
- Recursive assurance aggregation
- Overall assurance
- Dynamic infrastructure assessment
- Flexible object assessment

CoE_B	SP_1	SP_2	SP_3
AC_1	1	0	0
AC_2	1	1	0
AC_3	1	0	1

CoE_C	SP_1	SP_2	SP_3
AC_1	1	1	1
AC_2	1	1	0
AC_3	1	0	1

Assurance levels

Tree model:



CoE_B	SP_1	SP_2	SP_3
AC_1	**1**	**0**	**0**
AC_2	1	1	0
AC_3	1	0	1

CoE_C	SP_1	SP_2	SP_3
AC_1	**1**	**1**	**1**
AC_2	1	1	0
AC_3	1	0	1

	SP_1	SP_2	SP_3
CoE_B {AC_1}	1	1	1
CoE_C {AC_1}	1	1	0
CoE_B {AC_1} $\wedge$ CoE_B {AC_1}	**1**	**1**	**0**

Conclusion

- Strong security assessment framework for Cloud infrastructures is required
- Flexible
- Technology independent
- Both User and Provider centric
- Non invasive on the Cloud infrastructure

Thank you for your attention!

Contact

Aleksandar Hudic

AIT

0043 664 88390 711

aleksandar.hudic@ait.ac.at

AIT Austrian Institute of Technology • ETRA Investigación y Desarrollo • Fraunhofer Institute for Experimental Software Engineering IESE • Karlsruhe Institute of Technology • NEC Europe • Lancaster University • Mirasys • Hellenic Telecommunications Organization OTE• Ayuntamiento de Valencia • Amaris