The role of certification and standards for trusted Cloud solutions

A CloudWATCH webinar


CSA Cloud Bytes

Agenda

15:00 – Welcome and Introduction 10’

15:10 – The role of certification and standards for trusted cloud solutions 25’

15:35 – Open discussion 15’

15:50 – Questions from audience 10’

Introduction

Daniele Catteddu,

Managing Director, EMEA,

Cloud Security Alliance

Dr. Michaela Iorga,

Senior Security Technical Lead for Cloud Computing, NIST

NIST National Institute of Standards and Technology U.S. Department of Commerce

Marnix Dekker,
Security Expert
Information Security Officer,
ENISA

Claudio Belloli,

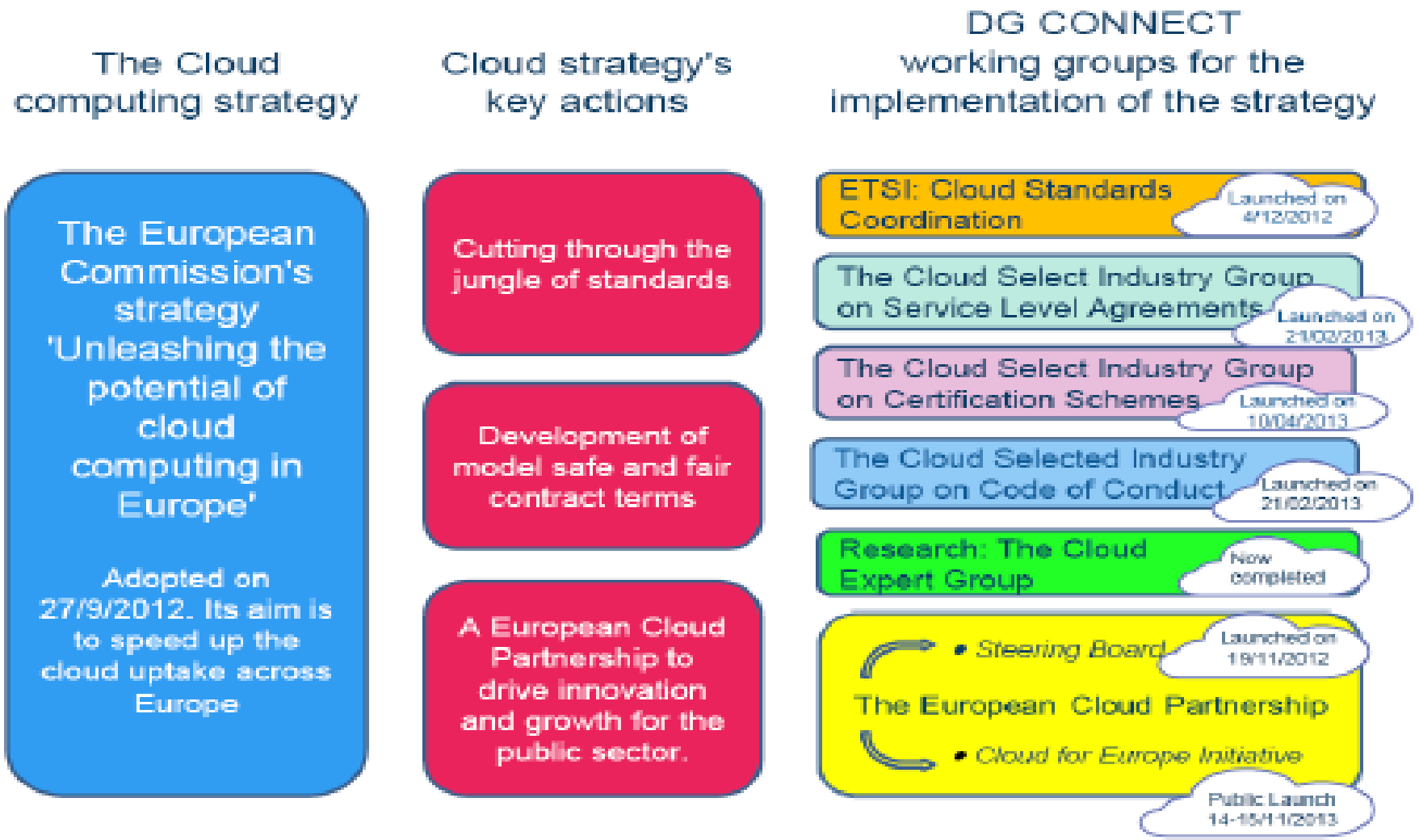
Information Systems Security Manager, GSA

Daniele Catteddu,

Managing Director, EMEA,

Cloud Security Alliance

European Cloud Strategy



Main conclusions:

- Standards situation is evolving rapidly and ETSI CSC's report can reflect only a snapshot in time.
- Cloud is not completely new: many standards used for cloud are not cloud specific, however they may still apply and will continue to evolve to reflect cloud scenarios.
- No jungle of standards, but jungle of fora!
- The SEC analysis shows the need for further standardization efforts in the area of accountability, cloud incident management and integration with legacy systems.

CERTIFICATION FOR CLOUD SERVICES

- In the Agenda of the EC
- Requested from Art29 WP as a measure for privacy compliance
- Already part of the cloud strategy in countries such USA, Singapore, Thailand, China, Honk Kong, Taiwan,
- In Europe various Member States are looking at a certification/accreditation schema for cloud service (especially in Public Procurement)
- The UK G-Cloud is based on a logic of companies accredited to offer service in the App Store

CERTIFICATION CHALLENGES

- Provide a globally relevant certification to reduce duplication of efforts
- Address localized, national-state and regional compliance needs
- Address industry specific requirements
- Address different assurance requirements
- Address “certification staleness” – assure provider is still secure after “point in time” certification
- Do all of the above while recognizing the dynamic and fast-changing world that is cloud

DEBATING AROUND CERTIFICATION FOR CLOUD

The debate around cloud certification has been based on the following key aspects:

- Suitability of existing security certification/Attestation schemes (e.g. ISO 27001 or SSAE16/SOC1-2-3) for the cloud market vs. the needs to introduce new schemes
- Mandatory vs. voluntary industry driven approaches
- Global vs. Regional/National schemes
- Cost
- Transparency
- Assurance and maturity/capability models

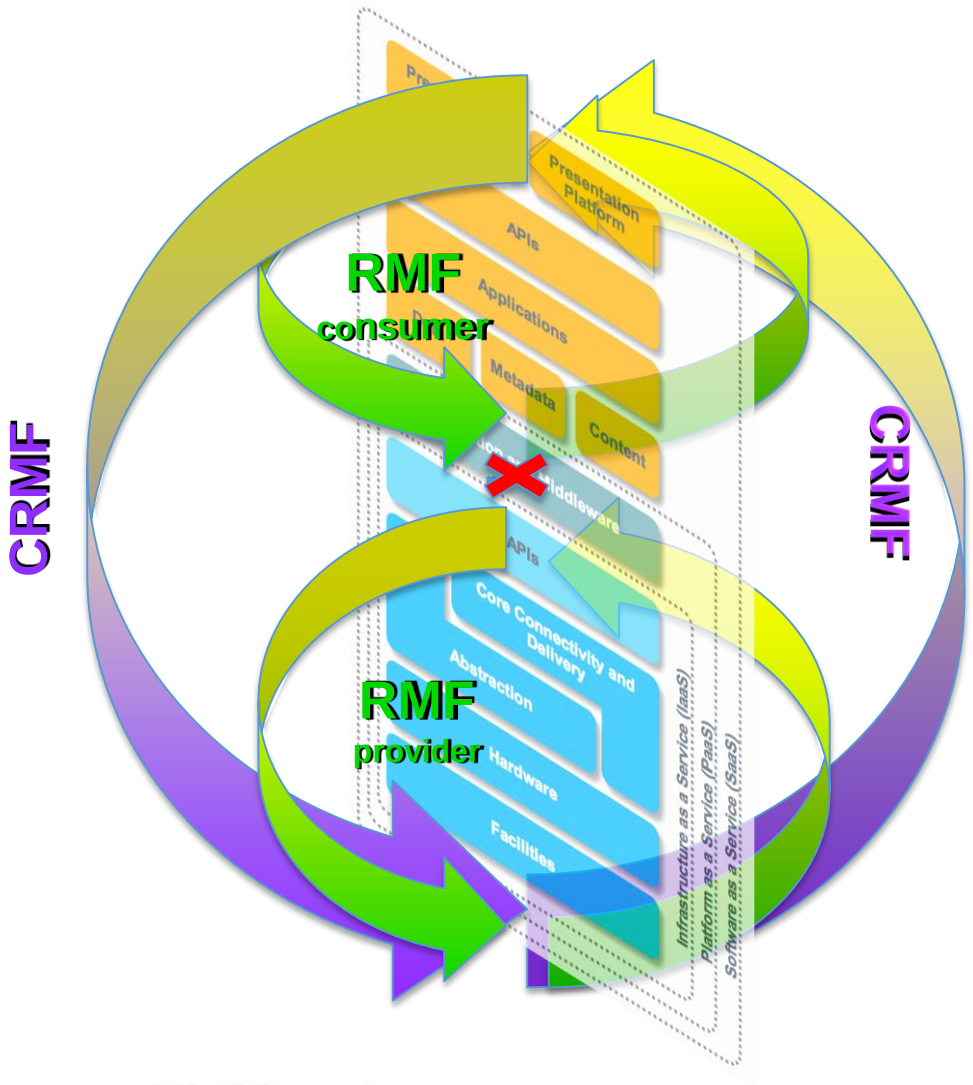
Dr. Michaela Iorga,

Senior Security Technical Lead for Cloud Computing, NIST

NIST National Institute of Standards and Technology U.S. Department of Commerce

When Dealing With an Iceberg Architecture…

Consumer's Risk Management in a Cloud Ecosystem



Risk Management Framework (SP 800-37 Rev1) :

Step 1: Categorize Information System
Step 2: Select Security Controls
Step 3: Implement Security Controls
Step 4: Assess Security Controls
Step 5: Authorize Information System
Step 6: Monitor Security Controls
(Repeat process as necessary)

Cloud-adapted Risk Management Framework (SP 800-173, draft):

Step 1: Categorize System to be migrated
Step 2: Identify Security Requirements, perform a Risk Assessment & select Security Controls
Step 3: Select best-fitting Cloud Architecture
Step 4: Assess Service Provider(s) & Controls
Step 5: Authorize Use of Service
Step 6: Monitor Service Provider [on-going, near-real-time] (Repeat process as necessary)

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Benefits of Assessment or Certification Programs

Step 4: Assess Service Provider's Security Controls

An A&A Program provides:

- *thorough,*
- *consistent,*
- *repeatable*

assessment processes!

UG Government Agencies are using FedRAMP

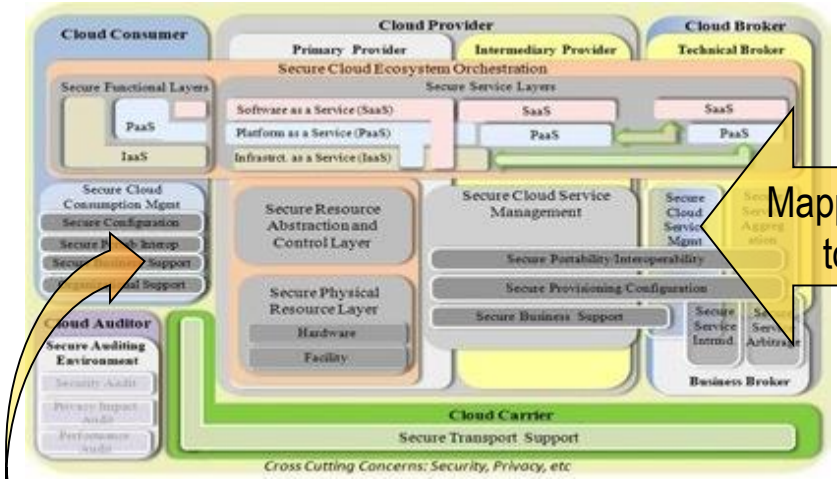
IMPORTANT to REMEMBER:

not all the controls are implemented the same

NIST National Institute of Standards and Technology U.S. Department of Commerce

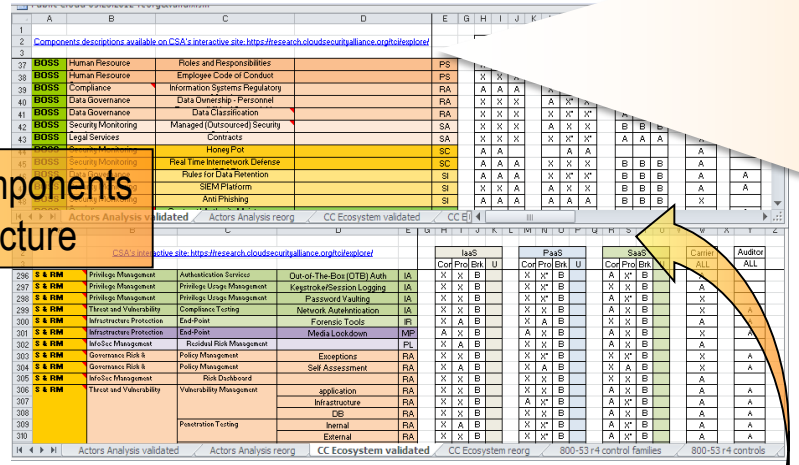
NIST CC Security Reference Architecture NIST SP 500-299

NIST Security Reference Architecture – formal model



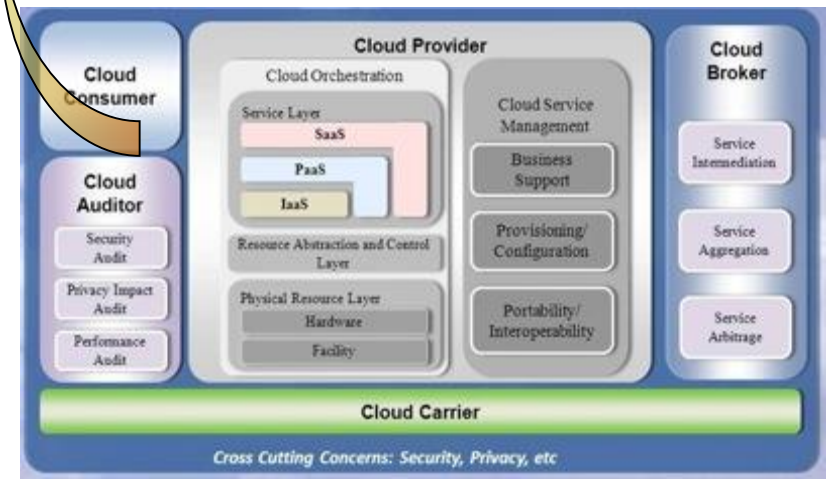
NIST Reference Architecture

NIST Security Reference Architecture – security components

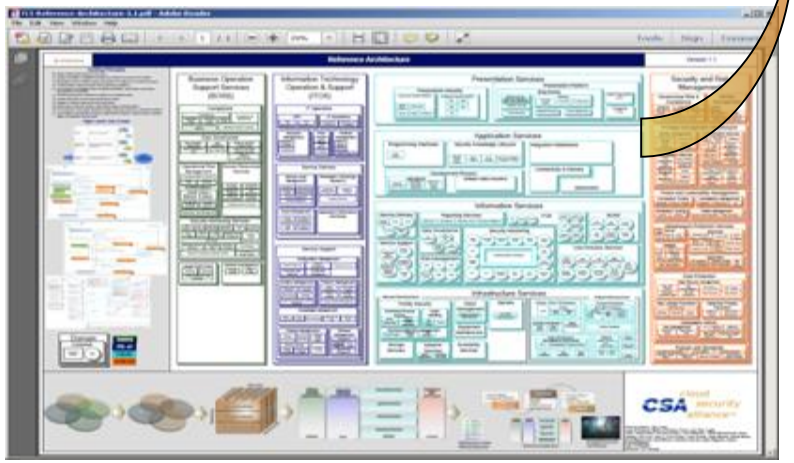


Mapping components to architecture

CSA's TCI Reference Architecture



+



NIST SP 800-53 R4 Security Controls

Low	Moderate	High
Configuration Management CM-1, CM-3, CM-5, CM-6, CM-11 Media Protection MP-1 Personnel Security PS-1 Physical And Env Protection PE-1 Planning PL-1 Risk Assessment RA-1, RA-2, RA-3, RA-5 Security Assessment And Authorization CA-2(1), CA-3(5) System And Communications Protection SC-16 System And Services Acquisition SA-3	Access Control IA-3, 4,5 Configuration Management CM-1, CM-3 (2), CM-5, CM-6, CM-11 Risk Assessment RA-1, RA-2, RA-3, RA-5 (1,2,5) Security Assessment And Authorization CA-2(2) System And Services Acquisition SA-8	Access Control AC2(1)(2)(3)(4)(5)(11)(12)(13) AC(6)(1)(2)(3)(5)(9)(10) AC(8),AC(10)AC(12), AC14), AC17, AC(18), AC19, AC21, AC-23, AC-24 Configuration Management CM-1, CM-3(1), CM-3(2), CM-5(1), CM-5(2), CM-5(3), CM-6(1), CM-6(2) CM-11 Risk Assessment RA-1, RA-2, RA-3, RA-5 (1,2,4,5) System And Services Acquisition SA-12, SA-17

NIST Cloud Computing Program

Where the Roads Could Merge

How Consumers can leverage different A&A Programs

NIST National Institute of Standards and Technology U.S. Department of Commerce

NIST Cloud Computing Program

Marnix Dekker,
Security Expert
Information Security Officer,
ENISA

About ENISA: Offices

Operational Office in Athens, Greece

Seat in Heraklion, Greece

About ENISA: Activities

Recommendations

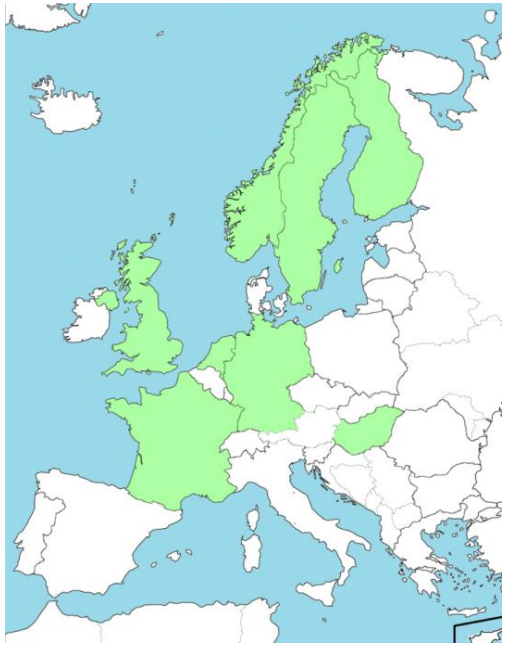
Policy Implementation

Mobilising Communities

Hands on

Example: National/Governmental CERTs in the EU

SITUATION IN 2005:



Finland
France
Germany
Hungary
The Netherlands
Norway
Sweden
United Kingdom

SITUATION IN 2014:

Armenia
Austria
Belgium
Bulgaria
Croatia
Czech Republic
Denmark
Estonia
Finland
France
Georgia
Germany
Greece
Hungary
Iceland
Ireland
Israel
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland
Turkey
Ukraine
United Kingdom
EU Institutions

See the CERT Interactive MAP: http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map

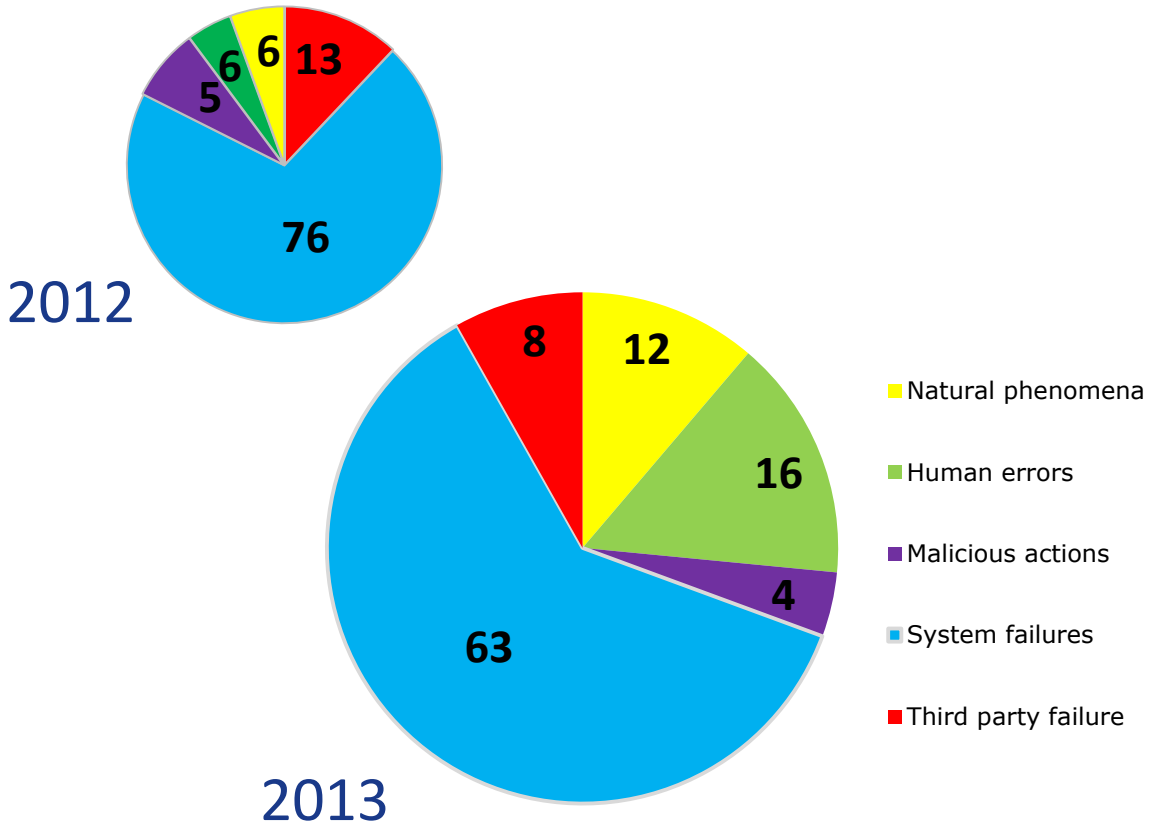
Example: EU Cybersecurity exercises

- Cyber Europe 2010
  - EU's first multinational cybersecurity exercise
  - Public sector agencies
- Joint EU-US Cybersecurity Exercise 2011
  - First transatlantic cooperation exercise
  - Table-top exercise - 'what-if' scenarios
- Cyber Europe 2012
  - Large scale realistic cyber-crisis exercise
  - Public and private sector involved
- Cyber Europe 2014
  - Just concluded – largest cyber exercise to date

More information on: http://www.enisa.europa.eu/c3e

Example: Security Breach Notification in the EU

- Annual reports about large outages in EU's telecoms



More information on http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting

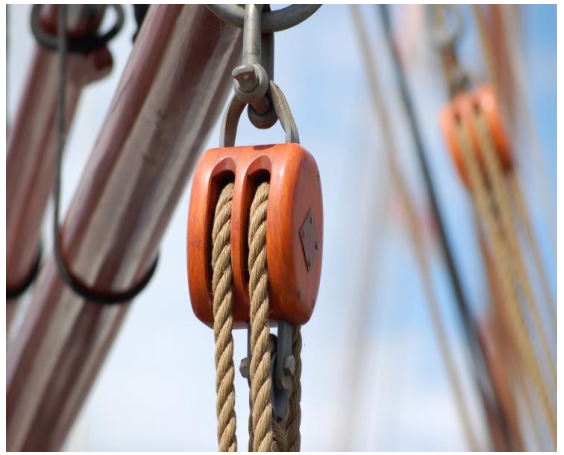
ENISA's Cloud Security work

- 2009 Cloud computing risk assessment
- 2009 Cloud security Assurance framework
- 2011 Security and resilience of GovClouds
- 2012 Procure secure (Security in SLAs)
- 2013 Critical cloud computing
- 2013 Incident reporting for cloud computing
- 2013 Securely deploying GovClouds
- 2013 Support EU Cloud Strategy
- 2013 Listing Cloud Certification schemes
- 2014 Cloud Certification Meta-Framework
- 2014 Security for GovClouds

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing

Security opportunities in cloud computing

- **Economies of scale**
  - ICT and security pros
  - 24/7 monitoring and incident response
  - Peak and DDoS protection
- **More standardized**
  - Formats, protocols
  - Portable, interoperable
  - Failover, backup
- **Security as a driver for cloud computing**
  - And not a barrier to adoption



ENISA supports the EU Cloud Strategy

- Motto: Harness the opportunities of cloud computing for the EU
- Legal framework should be cloud-friendly
  - DP reform proposal for more harmonized DP laws across the EU
- EU Cloud partnership and Cloud for Europe
  - Harmonize public sector procurement
  - Create better cloud solutions for the private sector also
- International collaboration
  - Many issues are global, not EU only
- Standards and certification
  - Support development of EU-wide voluntary certification schemes
  - Establish a list of such schemes by 2014.

Cloud Certification Schemes

- "list certification schemes relevant for cloud customers by 2014"
- CCSL
  - Provides an overview of, and information about certification schemes.
  - Aims to explain certification schemes to non-expert customers
- CCSM
  - Shows how common security requirements (used in the public sector) are met by existing certification schemes.
  - Aims to facilitate the use of certification schemes in public procurement
- Easier compliance is a cloud computing opportunity (via certification)
- Status:
  - CCSL is live at: https://resilience.enisa.europa.eu/cloud-computing-certification
  - Currently finalizing CCSM v1.0, an extension of CCSL.

Claudio Belloli,

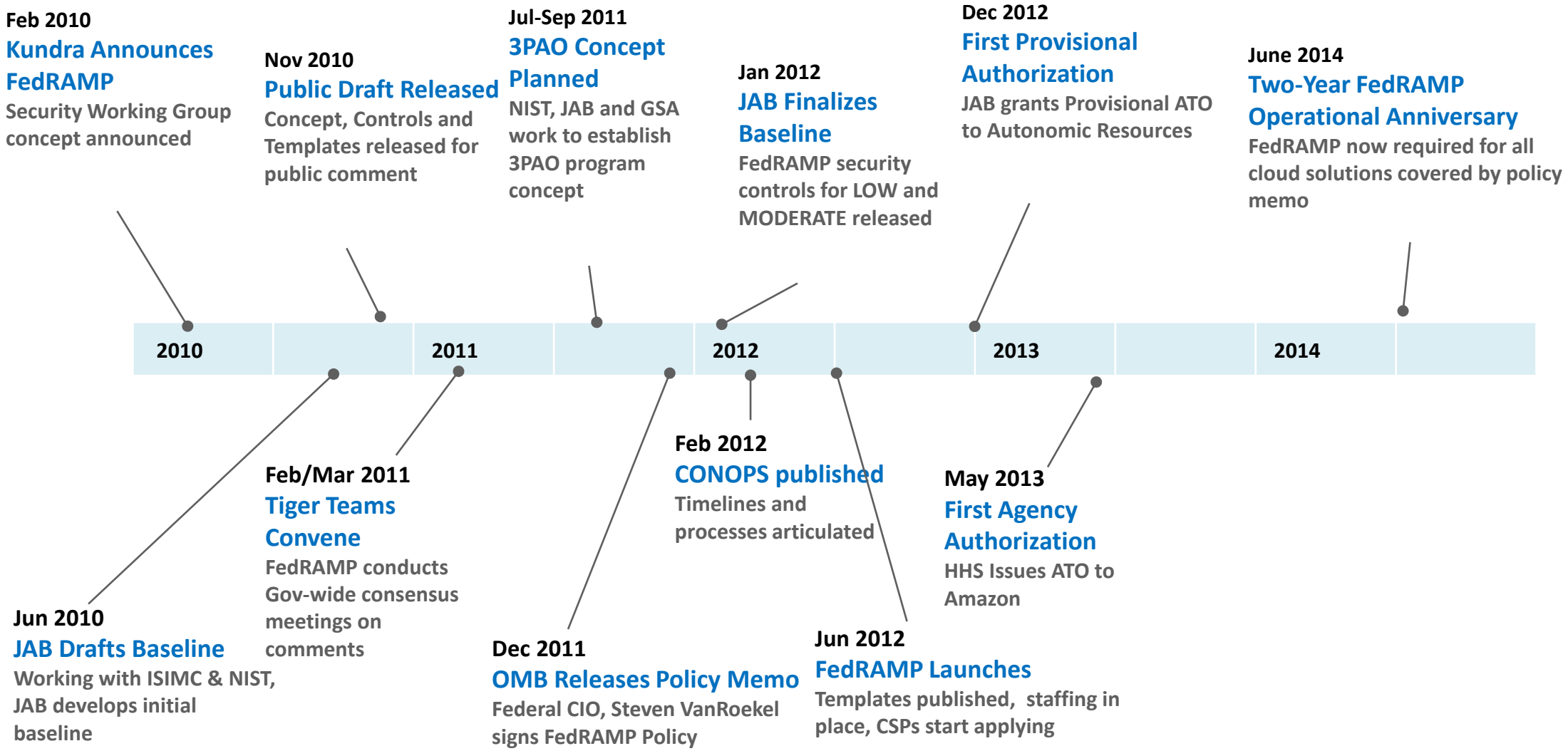
Information Systems Security Manager, GSA

FedRAMP

- What is FedRAMP?

Federal Risk and Authorization Management Program (FedRAMP) is a unified, government-wide risk management program focused on security for cloud-based systems. The program provides a standard approach for conducting security assessments of cloud systems based on an accepted set of baseline security controls and consistent processes that have been vetted and agreed upon by agencies across the federal government.

FedRAMP: A brief history



Impact of FedRAMP

Enables Cloud Security

- Successfully proven the U.S. government can securely use all types of cloud computing
- Created a standards based approach to security through risk management
- Implements continuous diagnostics and mitigation (CDM) for cloud
  - On-going visibility into CSP risk posture
  - Trend analysis of vulnerabilities and incidents
- Establishing a new marketplace for cloud vendors

Accelerates USG adoption of Cloud Computing

- Enables agencies achieve cost savings and efficiency through cloud computing
- Accelerates time to market for cloud services when authorizations re-used
  - DOI leveraged 6 authorizations and conservatively estimates a cost savings of 50% per authorization
  - HHS estimates cost savings at over $1M for their authorization and leveraging of Amazon alone

Ahead of the Curve

- Commercial industry is looking to FedRAMP as a model for building standards based security for cloud services
- Other countries are also looking to FedRAMP for their security frameworks

FedRAMP Key Stakeholders & Responsibilities

Federal Agencies

- Contract with Cloud Service Provider
- Leverage ATO or use FedRAMP process when authorizing
- Implement consumer controls

Cloud Service Provider

- Implement and document security
- Use Independent Assessor
- Monitor security
- Provide artifacts

FedRAMP PMO & JAB

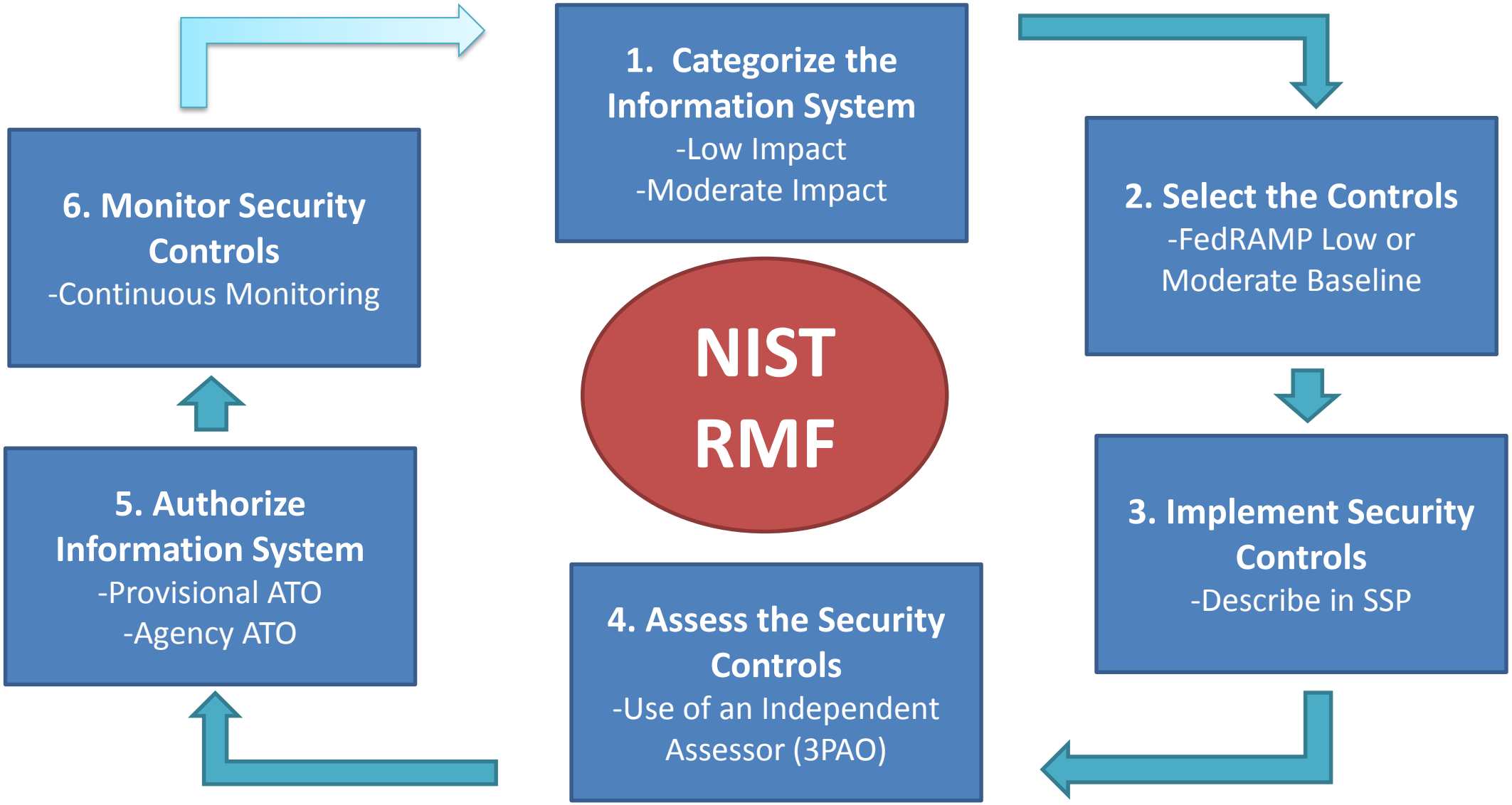
- Establish processes and standards for security authorizations
- Maintain secure repository of available security packages
- Provisionally authorize systems that have greatest ability to be leveraged government-wide

3PAOs

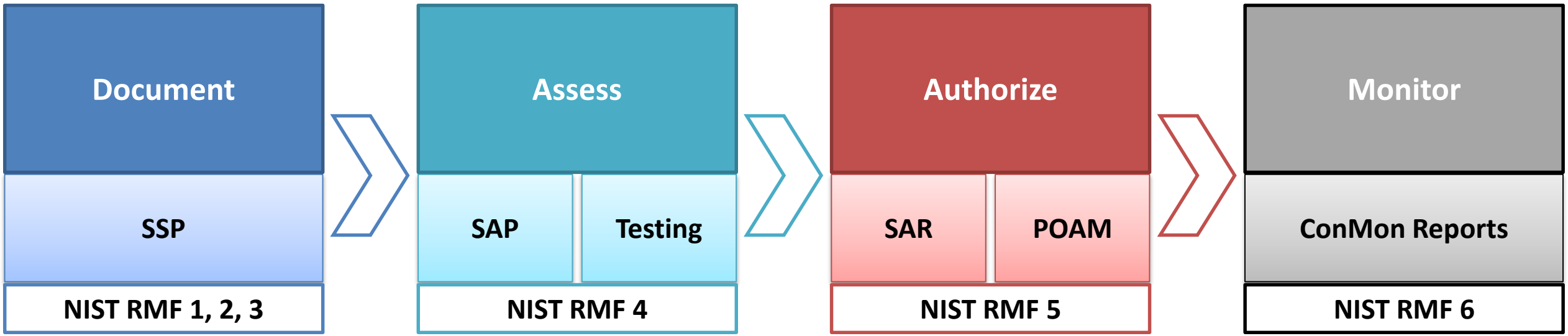
Third Party Assessment Organizations

- Cloud auditor, maintains independence from CSP
- Performs initial and periodic assessment of FedRAMP controls
- Does NOT assist in creation of control documentation

FedRAMP Relationship to the NIST Risk Management Framework



Timeline for Security Assessments



FedRAMP Authorization Paths

JAB Provisional Authorization (P-ATO)

- Prioritizes authorizing cloud services that will be widely used across government
- CIOs of DoD, DHS and GSA must agree that the CSP:
  - Strictly meets all the controls
  - Presents an acceptable risk posture for use across the federal government
- Conveys a baseline level of likely acceptability for government-wide use
- CSPs must use an accredited Third Party Assessor Organization (3PAO)
- FedRAMP PMO manages continuous monitoring activities; agencies review results

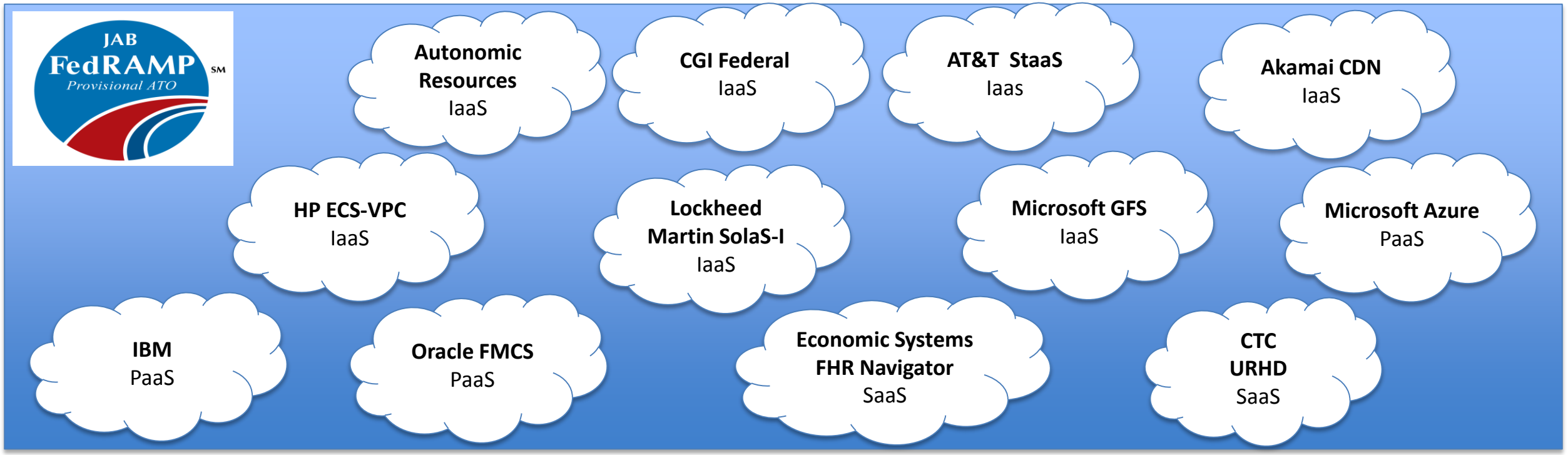
Agency ATO

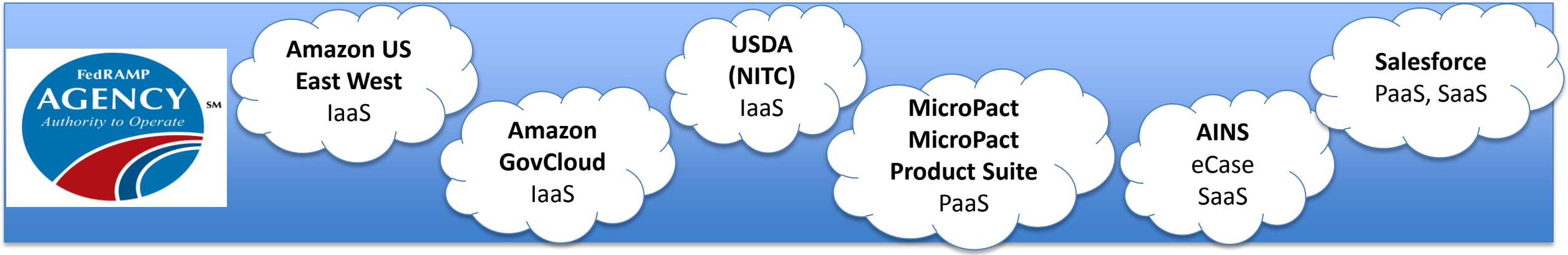
- Issued by the agency only
- Agencies have varying levels of risk acceptance
- Agency monitors the CSPs continuous monitoring activities
- Option to use a 3PAO or independent assessor to perform independent testing

CSP Supplied

- Submitted directly by CSP to FedRAMP
- CSP without ATO
- CSP must use an accredited 3PAO

Available P-ATOs and Agency ATOs





FedRAMP Security Controls Baseline

Security Controls Baseline Update

- Extensive public comment period
- PMO and JAB reviews

FedRAMP Baseline

Category of Changes	# Controls
Revision 3 Baseline	298
Withdrawn by NIST from Previous FedRAMP Baseline	*(41)*
Removed by Analysis FedRAMP Baseline	*(8)*
Not Selected in Rev. 4	*(4)*
Carryover Controls	245
Added by NIST	39
Added by analysis	41
Revision 4 Baseline	**325**

Federal Agency Responsibilities

- As of June 5, 2014, all cloud projects must meet the FedRAMP requirements when initiating, reviewing, granting, and revoking security authorizations
  - Use of FedRAMP security controls baseline
  - Use of mandatory templates
  - Provide FedRAMP PMO with ATO letters
  - Use FedRAMP repository for all ATOs where re-use is possible
- Agencies must enforce FedRAMP via contractual provisions
  - Template contract language available on FedRAMP.gov
  - Includes generic security section as well as control specific contract clauses
- Agencies must report to OMB via PortfolioStat cloud services that cannot meet FedRAMP requirements

Lessons Learned

CSP readiness tied to a number of factors

- Size of CSP infrastructure, alternate implementations, vulnerabilities or risks identified, type of service offering(s)
- Alignment of corporate business strategy to sell cloud services to the government
- Processes and procedures
- Able to address controls in preparation check list
  - Section 5.1 of the Guide to Understanding FedRAMP

For more information, please contact us or visit us the following website:

www.FedRAMP.gov
Email: info@fedramp.gov

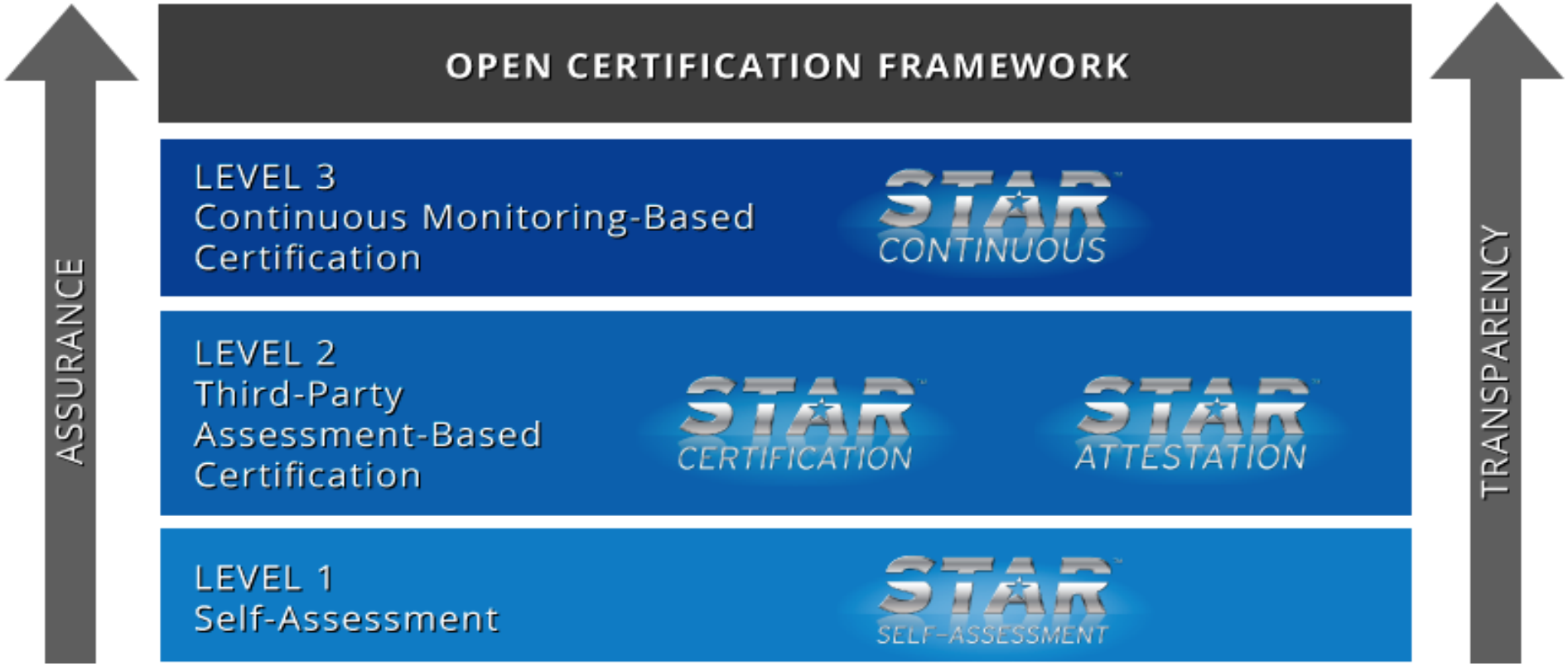
Follow us on twitter @ FederalCloud

Daniele Catteddu,

Managing Director, EMEA,

Cloud Security Alliance

OPEN CERTIFICATION FRAMEWORK



The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.

CSA STAR: SECURITY, TRUST & ASSURANCE REGISTRY

- Launched in 2011, the CSA STAR is the first step in **improving transparency and assurance** in the cloud.
- Searchable registry to allow cloud customers to review the security practices of providers, accelerating their due diligence and leading **to higher quality procurement experiences**.
- The STAR is a **publicly accessible** registry that documents the security controls provided by cloud computing offerings
- Helps users to assess the security of cloud providers
- It is based on a multilayered structure defined by **Open Certification Framework Working Group**

CCM: Cloud Control Matrix

- AIS Application & Interface Security
- AAC Audit Assurance & Compliance
- BCR Business Continuity Mgmt & Op Resilience
- CCC Change Control & Configuration Managemen
- DSI Data Security & Information Lifecycle Mgmt
- DSC Datacenter Security
- EKM Encryption & Key Management
- GRM Governance & Risk Management
- HRS Human Resources Security
- IAM Identity & Access Management
- IVS Infrastructure & Virtualization
- IPY Interoperability & Portability
- MOS Mobile Security
- SEF Sec. Incident Mgmt, E-Disc & Cloud Forensics
- STA Supply Chain Mgmt, Transparency & Accountability
- TVM Threat & Vulnerability Management

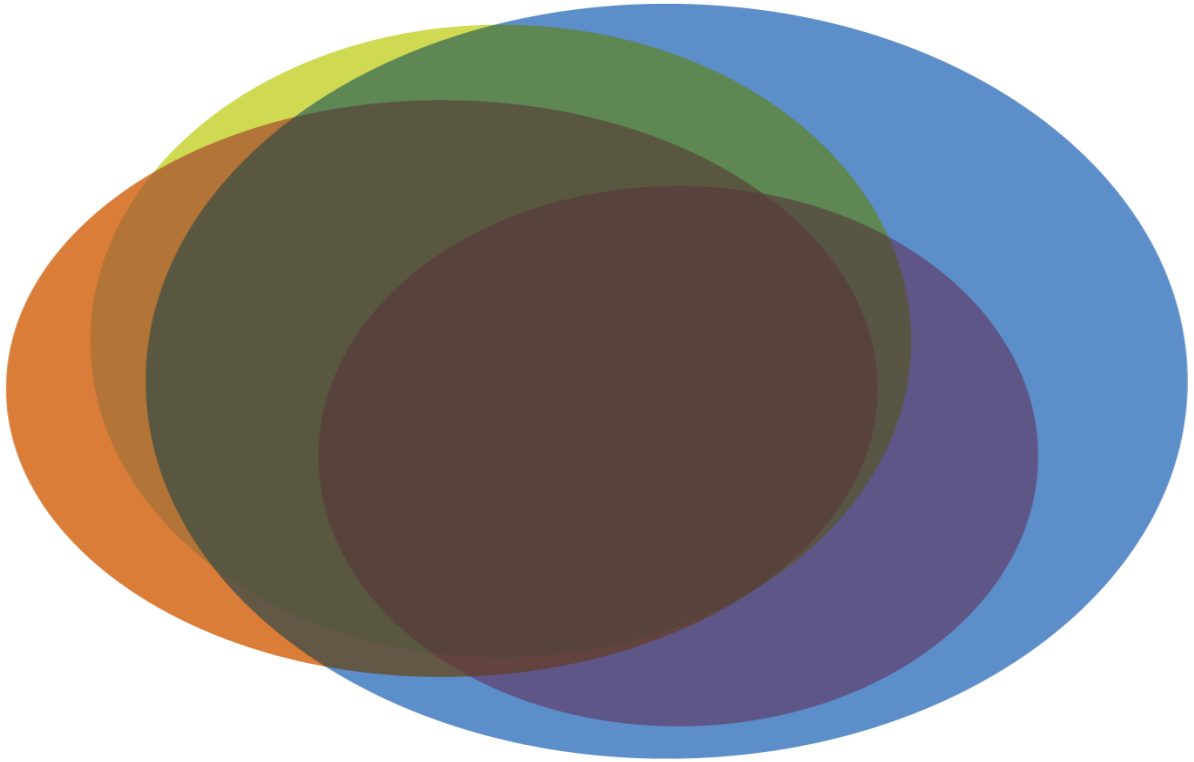
136 CONTROLS
Cloud Controls Matrix v3.0

//

133 CONTROLS
Cloud Controls Matrix v3.0.1

WHAT IS THE CCM?

- First ever baseline control framework specifically designed for Cloud supply chain risk management:
  - Delineates control ownership (Provider, Customer)
  - An anchor for security and compliance posture measurement
  - Provides a framework of 16 control domains
  - Controls map to global regulations and security standards
- Industry Driven Effort: 120+ Peer Review Participants
- Backbone of the Open Certification Framework and STAR

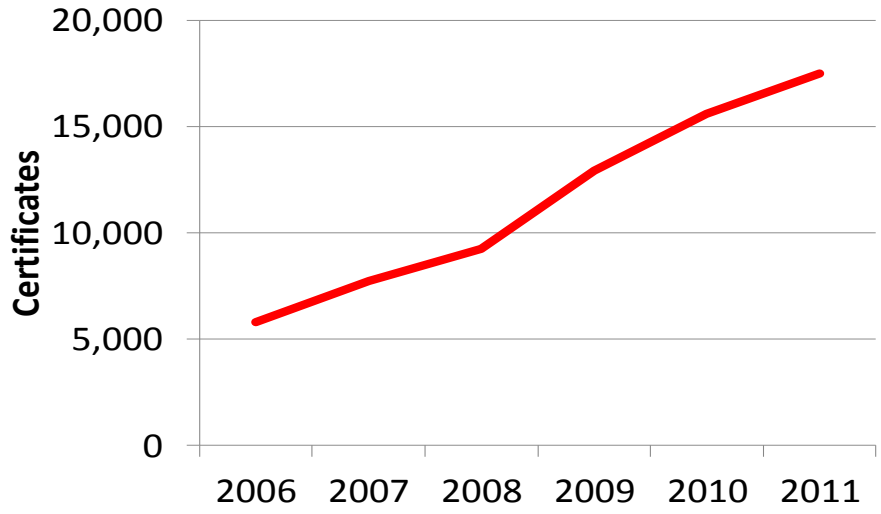


WHAT IS CSA STAR CERTIFICATION?

- The CSA STAR Certification is a **rigorous third-party independent assessment** of the security of a cloud service provider.
- **Technology-neutral** certification leverages the requirements of the **ISO/IEC 27001:2013** & the **CSA CCM**
- Integrates ISO/IEC 27001:2013 with the CSA CCM as **additional or compensating controls**.
- **Measures the capability levels** of the cloud service.
- Evaluates the efficiency of an organization's ISMS and ensures the scope, processes and objectives are "**Fit for Purpose."**
- Based upon the **Plan, Do, Check, Act** (PDCA) approach
- Enables the auditor to assess a company's performance, **on long-term sustainability and risks**, in addition to ensuring they are **SLA driven**.

CSA STAR CERTIFICATION & ISO 27001

- WHY CSA STAR Certification builds on ISO27001?
- Help organizations prioritize areas for improvement and lead them towards business excellence.
- ISO 27001 is the international standard for information security
- Considered as Gold Standard for information security
- There are over 17,500 organisations certified globally in over 120 countries.



MANAGEMENT CAPABILITY / MATURITY: SCORES

- When an Organization is audited a Management Capability Score will be assigned to each of the control areas in the CCM.
- This will indicate the capability of the management in this area to ensure the control is operating effectively.
- The management capability of the controls will be scored on a scale of 1-15. These scores have been divided into 5 different categories that describe the type of approach characteristic of each group of scores.

Score	Descriptor
1-3	No Formal Approach
4-6	Reactive Approach
7-9	Proactive Approach
10-12	Improvement Based Approach
13-15	Optimising Approach

APPROVING ASSESSORS

- They must demonstrate knowledge of the Cloud Sector
  - Either through verifiable industry experience – this can include though assessing organizations
  - Or through completing CCSK certification or equivalent
- They must be a qualified auditor working a ISO 27006 accredited CB
  - Evidence of conducting ISO 27001 assessments for a certification body accredited by an IAF member to ISO 27006 or their qualifications as an auditor for that organization.
- They must complete the CSA approved course qualifying them to audit the CCM for STAR Certification (This course will be carried out by BSI)

STAR ATTESTATION

- Star Attestation is a program under Level 2 of the CSA STAR Program that provides a framework for CPAs performing independent assessments of cloud service providers using AICPA SOC 2(SM) engagements supplemented by criteria in the CSA Cloud Controls Matrix (CCM). This assessment:
  - Is based on a mature attest standard to improve trust in the cloud and in the Information and Communication Technology (ICT) market by offering transparency and assurance.
  - Allows for immediate adoption of the CCM as additional criteria and the flexibility to update the criteria as technology and market requirements change.
  - Does not require the use of any criteria that were not designed for, or readily accepted by cloud providers.
  - Provides for robust reporting on the suitability of the design and operating effectiveness of a service organization's controls relevant to security and availability based on criteria in the AICPA's Trust Services Principles and Criteria and the CCM.

IN SUMMARY

- Transparency, assurance and accountability are the key elements to increase trust in cloud computing
- Security certifications could be good tool to increase trust, ONLY if:
  - Auditors are qualified and properly certified
  - The control framework used as underlying standard is relevant
  - The control framework is publicly available and it's capability to address requirements can be verified.
  - Scheme support transparency (e.g via publication of scope and SoA)
  - Different assurance need are supported (e.g. self-certification, 3rd-party assessment, continuous monitoring).
- Certifications need to be affordable for Small and Medium companies
- CSA Open Certification Framework and STAR Certification/Attestation provides all the above.

Open discussion

THANK YOU!

cloudwatchhub.eu