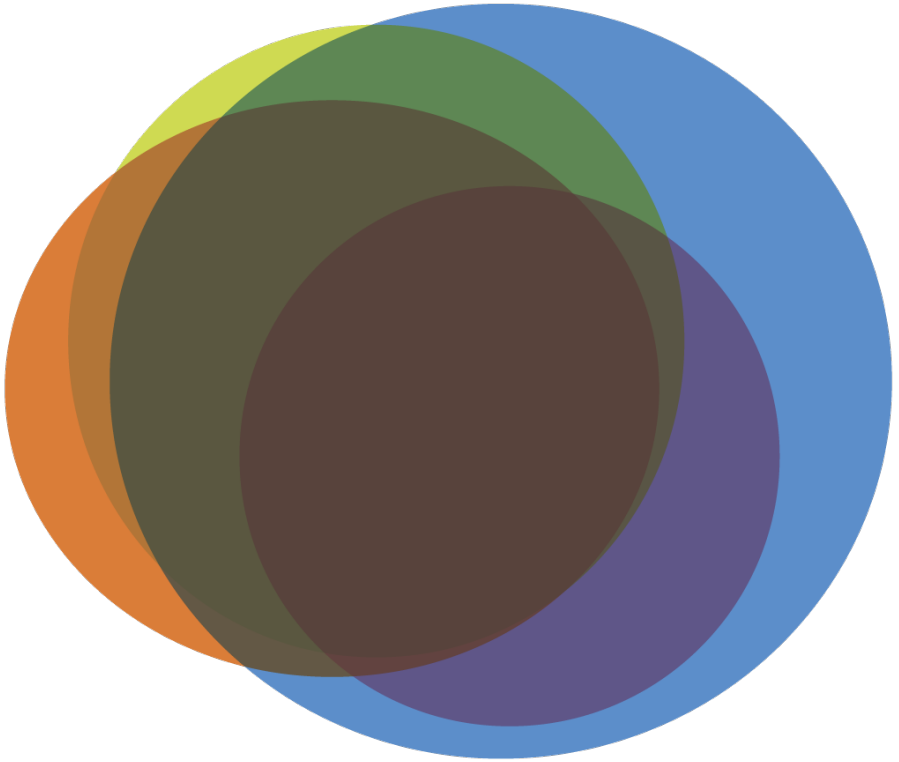
Towards a Financial Service Stakeholder Platform for Cloud Security (FSSP)



Dr. Jesus Luna Garcia
Director of Research
Cloud Security Alliance (Europe)

Agenda

- Cloud Security Alliance (CSA)
- CSA Financial Service Stakeholder Platform (FSSP)
- How to Build Trust in Cloud Computing?

ABOUT THE CLOUD SECURITY ALLIANCE

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

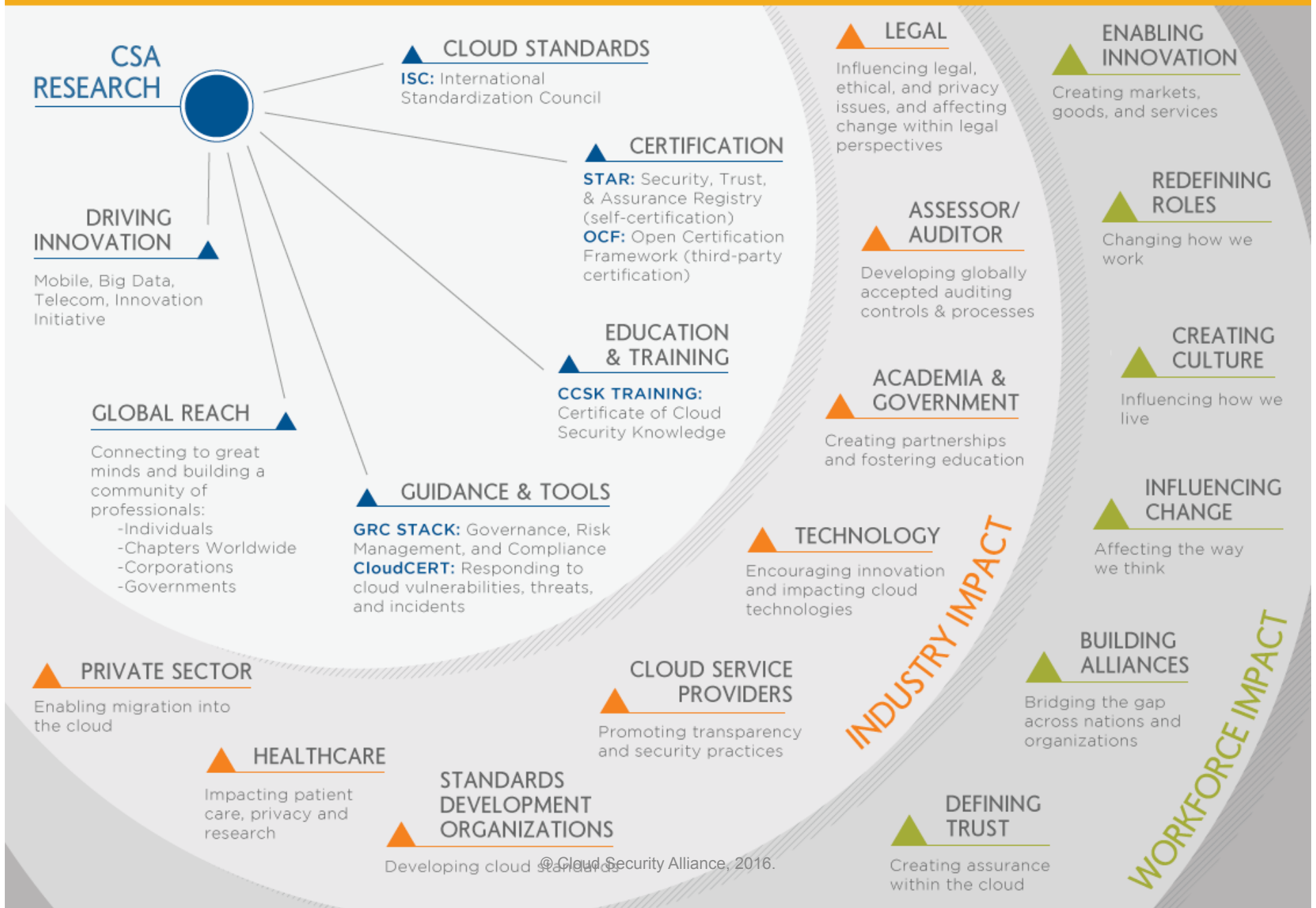
- Global, not-for-profit organization
- Over 70,000 individual members, more than 300 corporate members, and 65 chapters
- Building best practices and a trusted cloud ecosystem
  - Agile philosophy, rapid development of applied research
  - GRC: Balance compliance with risk management
  - Reference models: build using existing standards
  - Identity: a key foundation of a functioning cloud economy
  - Champion interoperability
  - Enable innovation

ABOUT THE CLOUD SECURITY ALLIANCE

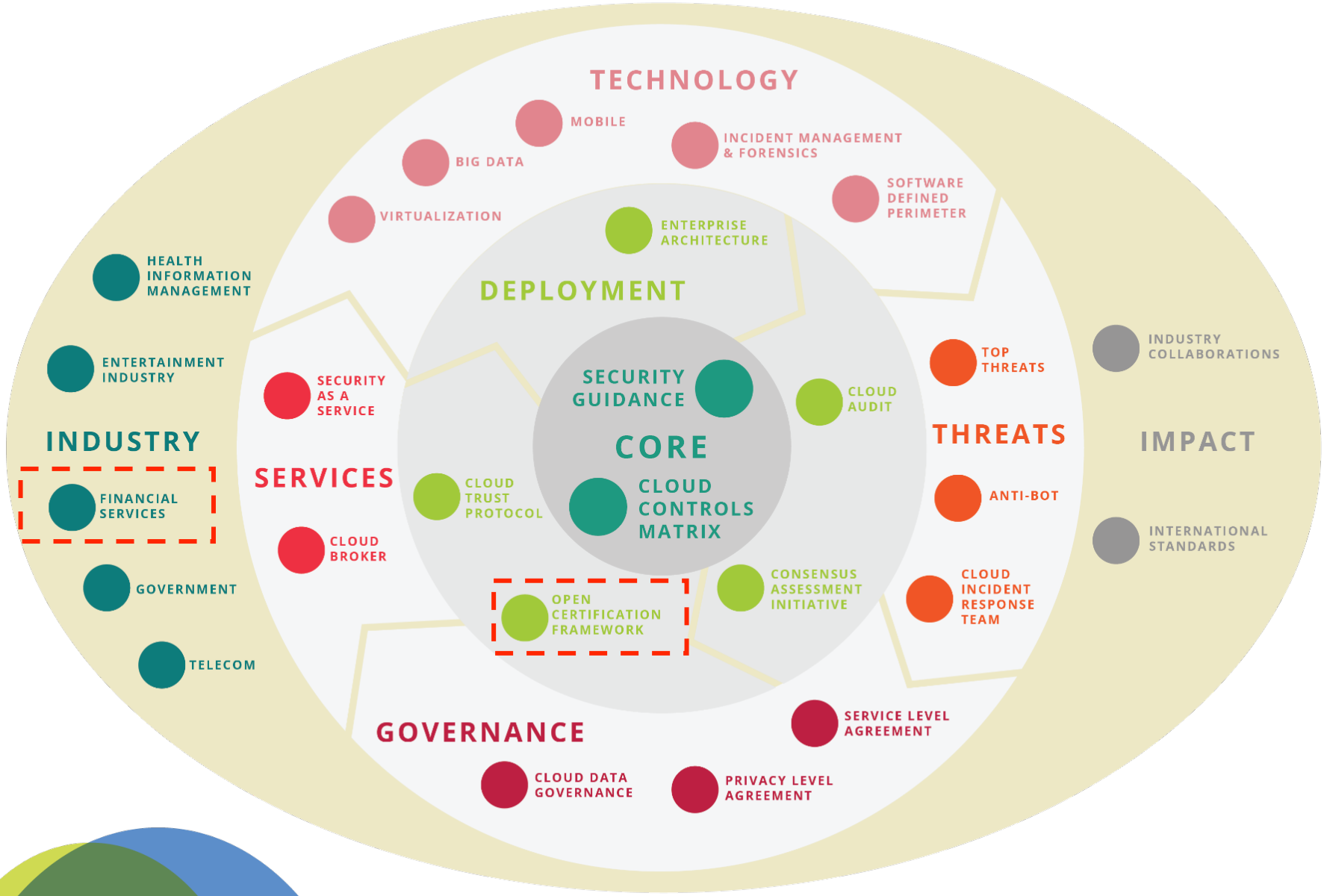
"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

- RESEARCH
  - https://cloudsecurityalliance.org/research/
- ADVISE GOVERNMENTS AND PRIVATE COMPANIES
- EDUCATION – PROFESSIONAL CERTIFICATION – TRAINING
  - https://cloudsecurityalliance.org/education/
- PROVIDER CERTIFICATION
  - https://cloudsecurityalliance.org/star/
- STANDARDS
  - https://cloudsecurityalliance.org/isc/
- Events
  - https://cloudsecurityalliance.org/events/

IMPACT OF CSA RESEARCH



CSA Research Portfolio



CSA & Financial Sector: Background

- CSA decided in 2013 to start focusing on critical sectors and to develop best practices tailored to the specific needs of these vertical markets.
  - The Financial Sector was identified as a priority
- In 2014 the CSA Financial Services Working Group was launched
- In 2015 CSA published the survey report: “How Cloud is Being Used in the Financial Sector”
- In 2015 CSA authored an EU Agency for Network and Information Security (ENISA) study ”Secure Use of Cloud Computing in the Finance Sector”
- Currently CSA has 28 corporate members from the Financial Sector

“How Cloud is Being Used in the Financial Sector” Survey Report

- Key Findings:
  - As cloud computing becomes more prevalent throughout the financial sector, a mixed strategy of leveraging both private and public clouds emerge as the norm for most businesses
  - Most organizations do not have a concerted cloud migration strategy
  - Data protection is a preeminent security concern for the financial sector moving to the cloud. In particular, data protection standards and relevant laws are “top of mind” to our survey respondents.
  - Industry regulation drives compliance requiring financial institutions to implement specific security measures to consider migrating to cloud services.
- https://cloudsecurityalliance.org/download/cloud-adoption-in-the-financial-services-sector-survey/

CSA Financial Service Stakeholder Platform (FSSP)

FSSP's Objectives

1. Global best practices and de-facto standards in the areas of cloud governance and risk management
2. Regional (EU, APAC, Americas) and global mechanisms for security and privacy compliance
3. Global best practices and de-facto standards for incident management and information sharing
4. Technical solutions that can improve the security capabilities of the financial sectors
5. Recommendations addressed to policy makers and regulators
6. Awareness and educational materials addressed to regulators, financial service risk/security/compliance/audit officers, and cloud service providers

FSSP: Membership

Eligible members are:

- CSA enterprise customer corporate members operating in the financial institution sector (FIs)
- CSA solution provider corporate members (CSPs)
- Financial service regulators / supervisory authority / central banks (Regulators), and other relevant organizations (DPA, Agencies, etc.)

FSSP Action plan for Y1 (draft) - Best practices for cloud security in the Financial Sector (1/3)

- Guidelines on how to effectively manage risks in the cloud, and how to take advantage of the security opportunities
  - **Task 1**: Collection and review of international good practices and (de-facto) standards in the areas of cloud governance and risk management
    - EU
    - USA
    - APAC
  - **Output 1**: Collection of standards, good practice and requirements for governance and risk management - **Q2/2016**
  - **Task 2**: Collection and review of good practices and de-facto standards for incident management and information sharing
    - EU
    - USA
    - APAC
  - **Output 2**: Collection of standards, good practice and requirements for incident management and information sharing - **Q2/2016**

FSSP Action plan for Y1 (draft) - Best practices for cloud security in the Financial Sector (2/3)

- Guidelines on how to effectively manage risks in the cloud, and how to take advantage of the security opportunities
  - **Task 3**: Identification of security and privacy requirements
    - EU
    - USA
    - APAC
  - **Output 3**: Security and privacy controls for the cloud in financial sector - **Q4/2016**
  - **Task 4**: Development of guidelines for risk assessment/cloud strategy
  - **Output 4**: Guidelines for risk assessment in the cloud - **Q4/2106**

FSSP Action plan for Y1 (draft) - Best practices for cloud security in the Financial Sector (3/3)

- Educational papers for financial sector in the cloud
  - **Task 5**: Information campaign on CSP transparency & assurance (target audience: Regulators)

  - **Output 5**: Architectures and deployment models - **Q2/2016**
  - **Output 6**: Service Level Management - **Q3/2016**
  - **Output 7**: Certification & Assurance - **Q4/2016**

FSSP Action plan for Y1 (draft) - Best practices for cloud security in the Financial Sector (3/3)

- Educational papers for financial sector in the cloud
  - **Task 5**: Information campaign on CSP transparency & assurance (target audience: Regulators)

  - **Output 5**: Architectures and deployment models - **Q2/2016**
  - **Output 6**: Service Level Management - **Q3/2016**
  - **Output 7**: Certification & Assurance - **Q4/2016**

How to Build Trust in Cloud Computing?

Trusted IT means…	What it means for CSA…
Ensuring Availability Of Applications, Systems & Data Continuous Monitoring	Security Service Level Agreements
Protecting Data Data-centric solutions	Continuous monitoring-based certification
Identifying & Repelling Threats Advanced Security (Automation)	Adoption of standards

What is a cloud security SLA?

- "*Contract*" which describes the *Service*, the associated security *quality* levels (SLOs/SQOs) and specifies the security *metrics* to be implemented by the Provider.

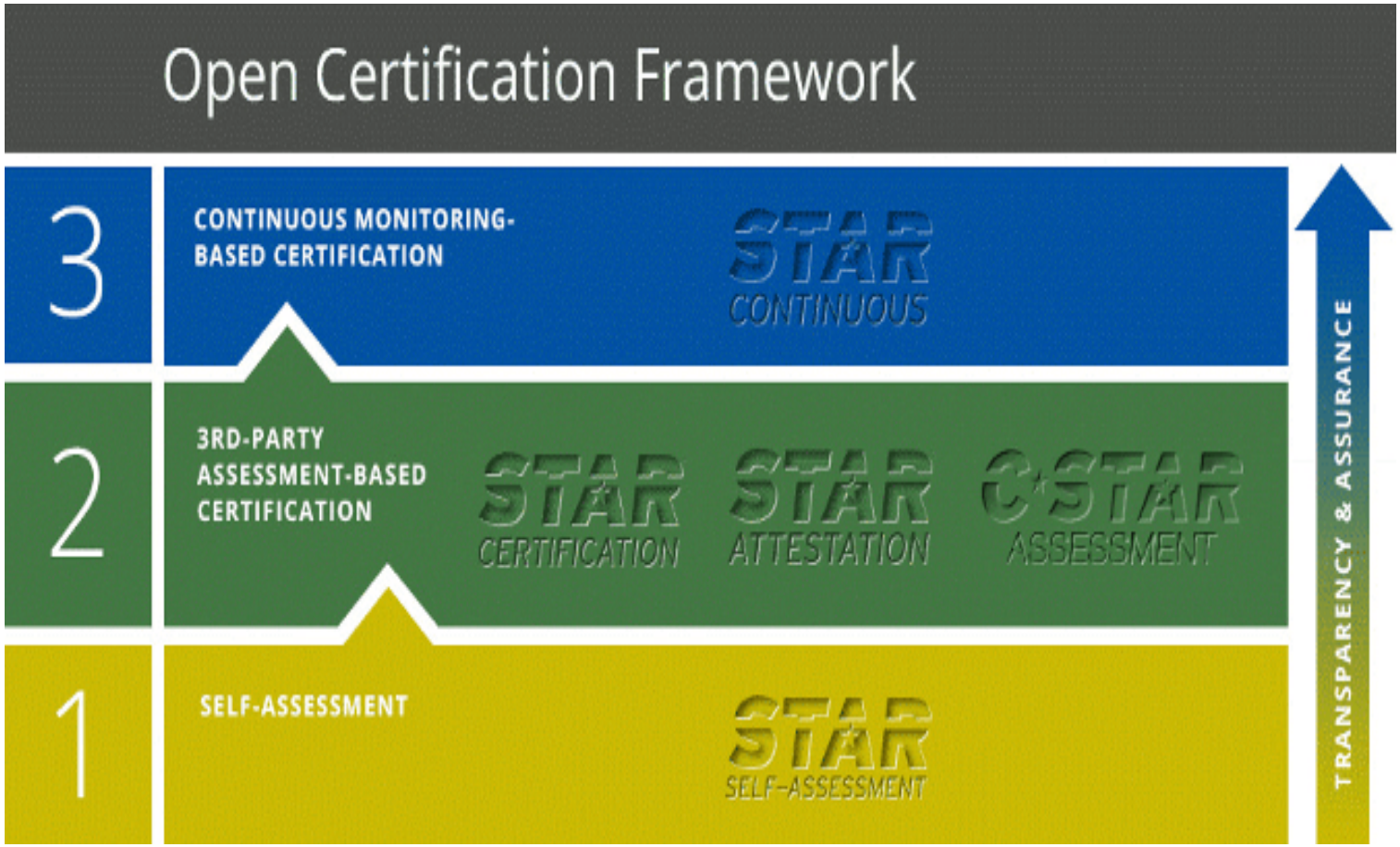
Advantages:

- Security automation
- Transparency
- Trust!

Are you SLA-Ready *? Find it out in http://www.sla-ready.eu/*

Making Cloud SLAs readily usable in the EU private sector

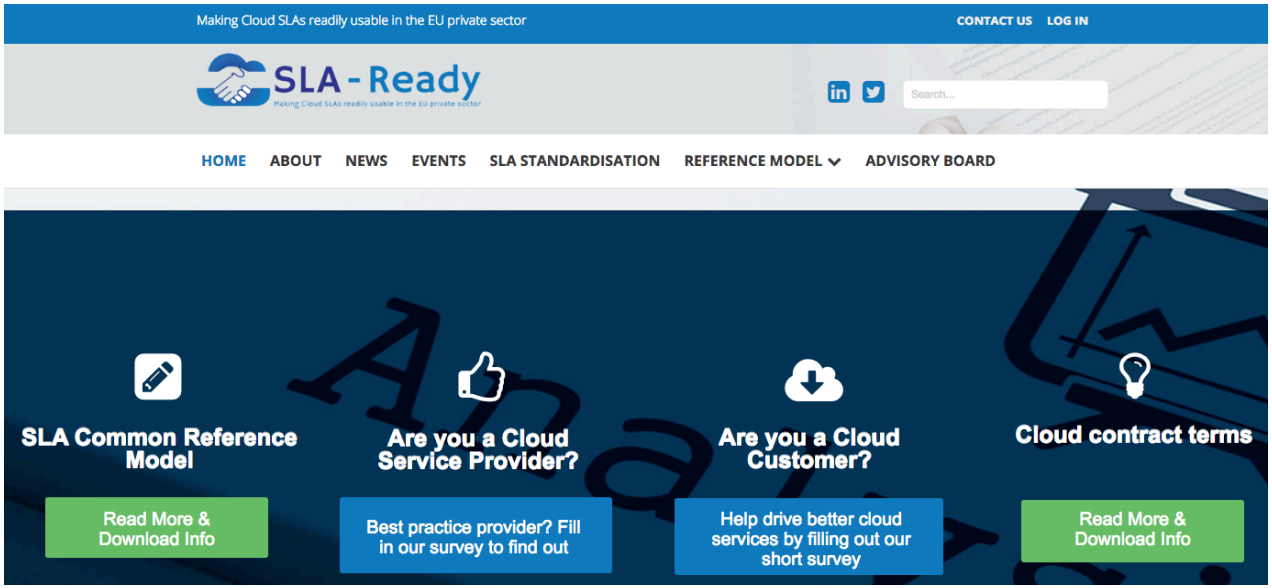
The role of cloud security certification



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

Are you SLA-Ready?
http://www.sla-ready.eu/

- Cloud SLAs are not standardized nor easy to use by SMEs.
- The EU project SLA-Ready aims to empower SMEs through a set of best practices and tools, including a Common Reference Model.
- Be part of it and let's know your opinion!



Cloud Standards

ISO/IEC 17788: Cloud computing – Vocabulary and overview

- Collaborative Team (CT) with ITU-T/SG13 to develop common text
- Defines key cloud terminology and provides an overview of cloud computing
- Intended to be a foundation document for cloud computing

ISO/IEC 17789: Reference architecture

- Collaborative Team (CT) with ITU-T/SG13 to develop common text
- Covers general concepts and characteristics of cloud computing, the
- components/functions and roles and their capabilities and inter-relationships

Cloud standards (Cont'd)

ISO/IEC 27017: Code of practice for information security controls for cloud computing services based on ISO/IEC 27002

- Common text standard with ITU-T/SG17
- Additional implementation guidance for relevant information security controls specified in ISO/IEC 27002;
- Additional controls and implementation guidance that specifically relate to cloud computing services.

ISO/IEC 27018: Code of practice for data protection controls for public cloud computing services

- Applies to organizations providing public cloud computing services that act as PII processors (possibly PII controllers)
- Establishes commonly accepted control objectives, controls and guidelines for implementing controls

Cloud standards (Cont'd)

ISO/IEC 19086-1/-4: Cloud SLAs

- Provides terminology and components of SLAs for cloud services (including security and privacy)
- Specifies a model for describing cloud SLA metrics
- Presents the core/conformance requirements associated provided SLA components
- Facilitates common understanding between the Cloud Service Providers and the Cloud Service Customers

THANK YOU!

CONTACT US

Jesus Luna, Research Director

Europe, Cloud Security Alliance

Twitter: @jlunagar

@CloudSA

jluna@cloudsecurityalliance.org