

The CSA Open Certification Framework & STAR Program

Damir Savanovic,
Senior Analyst & Researcher
Cloud Security Alliance



A large blue circle containing the text 'ABOUT THE CLOUD SECURITY ALLIANCE' in white, bold, uppercase letters.

ABOUT THE CLOUD SECURITY ALLIANCE

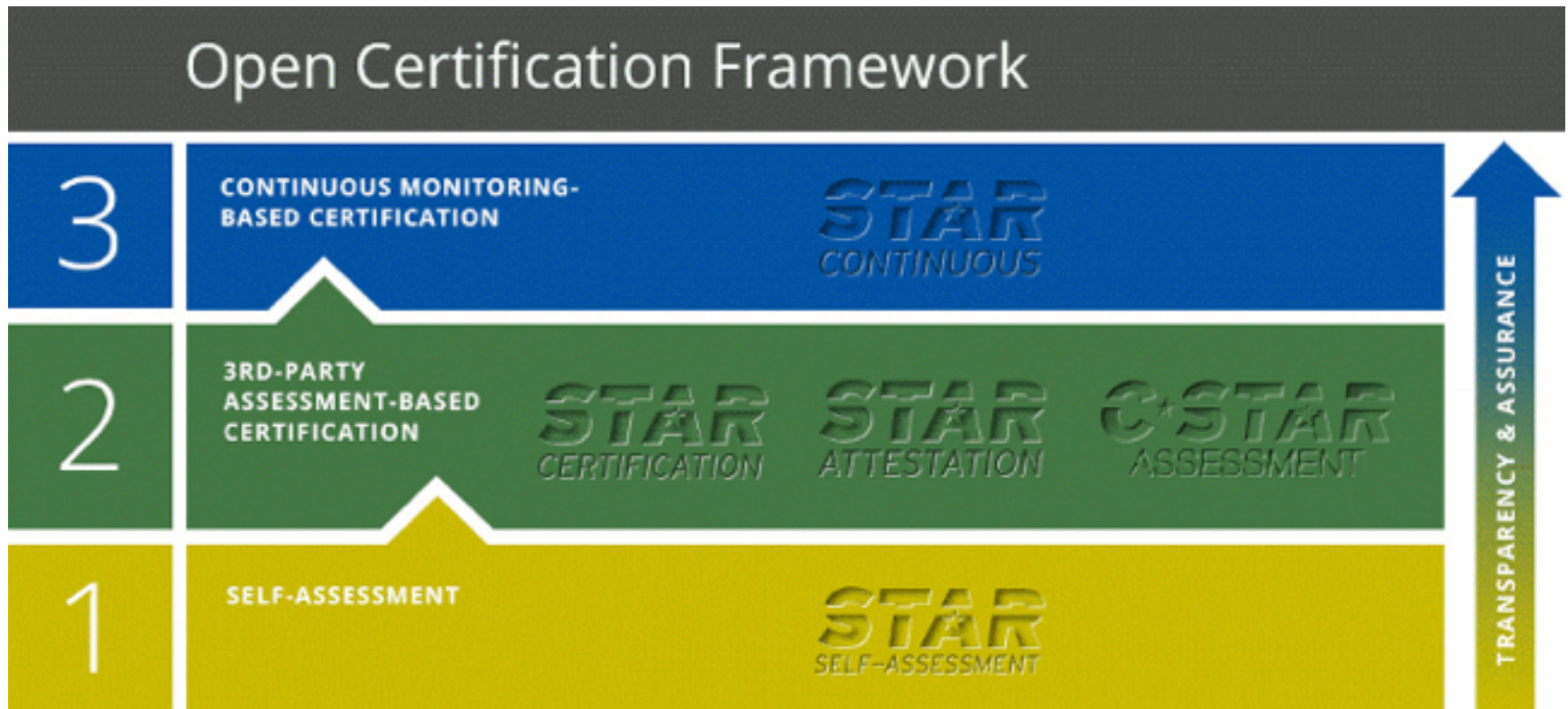
“To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”

- 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
 - Advocacy of prudent public policy

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

OPEN CERTIFICATION FRAMEWORK



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



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**.

HOW IT PROVIDES ASSURANCE TO CLIENTS?

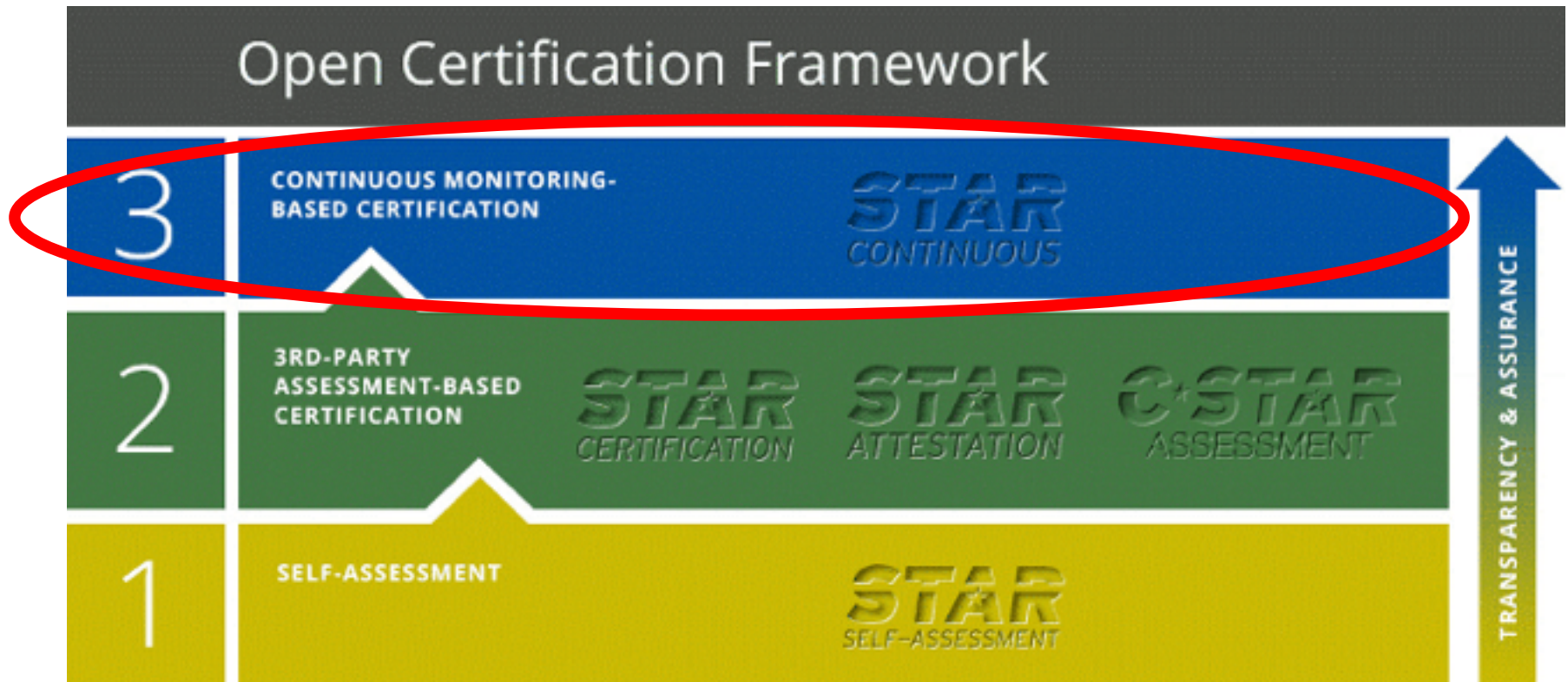
- ISO 27001 requires the Organization to evaluate their customers' requirements and expectation, and contractual requirements. It requires that they have implemented a system to achieve this.
- ISO 27001 requires the Organization has conducted a risk analysis that identifies the risks to meeting their customer's expectations.
- The Cloud Controls Matrix requires the Organization to address the specific issues that are critical to cloud security.
- The maturity model assesses how well managed activities in the control areas are.



Current level of adoption

- Currently 152 Cloud Service Providers Word Wide have decided to be part of the STAR Program!
- That includes companies with either STAR Self Assessment (115) or STAR Certification (31), C-STAR Assessment (3) or STAR Attestation (3)

OPEN CERTIFICATION FRAMEWORK



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

OCF Level 3



- CSA STAR Continuous is meant to enable automation of in the auditing/assessment/monitoring (either internal or external) and certification of security practices of CSPs. CSP will share their security practices according to CSA formatting and specifications, and customers, broker and tool vendors can retrieve and present this information in a variety of contexts.
- It builds on the following CSA best practices/standards:
 - Cloud Control Matrix (CCM)
 - Cloud Trust Protocol (CTP)
 - CloudAudit (A6)
 - CSA Cloud Security SLAs



What do we want to monitor/audit

- In the field of security, the notion of “continuous monitoring” has been applied both to high-level “control objectives”, “controls” or lower-level objects such as “service level objectives”, “performance indicators” and “security properties”.
- In the context of CSA STAR Continuous we want to monitor:
 - Control Objectives (i.e. CCM controls) and
 - *Security Attributes* as related to Service Level Objectives.

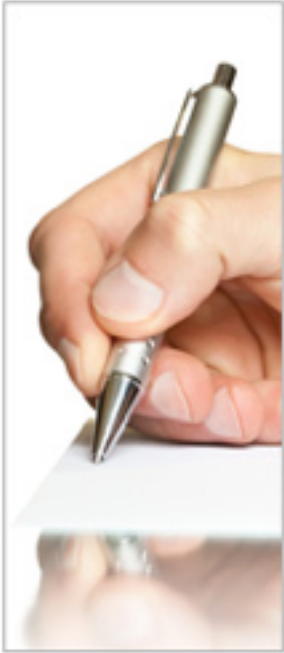


Privacy Level Agreement - PLA V2

Compliance Tool



DPA's opinions on PLA?



I think [the PLA Outline] is a very helpful document, both for potential customers of CSPs and for CSPs themselves.

By following closely the WP29 Opinion it ensures that both parties understand the obligations under EU law - probably the strictest requirements they will have to comply with.

Hopefully it will be accepted by CSPs that, if they want to be viewed as acceptable service providers - especially by EU-based organisations - they are going to have to be able to answer successfully the questionnaire that is annexed to the document.

**Billy Hawkes,
Irish Data Protection Commissioner**

Transparency and information are key to build trust in the cloud ecosystem.

This is why the CNIL has actively contributed to the elaboration of the PLA-outline.

As it gets gradually adopted by CSPs, it will become an important building block for constructing a modern ethical and privacy-preserving framework, adequate to the challenges that face all stakeholders in the digital world.

**Isabelle Falque-Pierrotin,
President of the CNIL**

Privacy Level Agreement V2

1. Identity of the CSP (and of representative in the EU as applicable), its role, and the contact information for the data protection inquiries
2. Ways in which the data will be processed
3. Data transfer
4. Data security measures
5. Monitoring
6. Personal Data breach notification
7. Data portability, migration, and transfer back assistance
8. Data retention, restitution, and deletion
9. Accountability
10. Cooperation
11. Legally required disclosure





CSA *2015 EMEA* Congress

November 17 - 19, Berlin, Germany

Udo Helmbrecht, Bruce Schneier, Radu Popescu-Zeletin, Isabelle Falque-Pierrotin, Matthew Goodrich and Pearse O'Donohue have been confirmed as keynote speakers.





THANK YOU!

CONTACT US

Damir Savanovic; Senior Analyst &
Researcher, Cloud Security Alliance

Twitter: @DamirSavanovic

@CloudSA

dsavanovic@cloudsecurityalliance.org

star-help@cloudsecurityalliance.org

<https://cloudsecurityalliance.org/star/>