EUROPEAN COMMISSION
DIRECTORATE-GENERAL INFORMATICS

Directorate R – Change Management & Resources
DIGIT R3 - ICT Procurement & Contracts

# DYNAMIC PURCHASING SYSTEM FOR CLOUD SERVICES

REFERENCE

**DIGIT/A3/PR/2018/035**
**CLOUD II DPS 1**

# ANNEX V

# SECURITY FRAMEWORK

EUROPEAN COMMISSION
DIRECTORATE-GENERAL INFORMATICS

Directorate C - Digital Workplace & Infrastructure
DIGIT C1 - Cloud & Service Management Capabilities

# DYNAMIC PURCHASING SYSTEM FOR CLOUD SERVICES

REFERENCE
**DIGIT/A3/PR/2018/035**
**CLOUD II DPS 1**

—

## ANNEX V

# SECURITY FRAMEWORK

## TABLE OF CONTENTS

## 1. Introduction

This document defines **Security Objectives** relevant for the provision of Cloud services requested in this procedure. These security objectives are based on the ENISA Cloud Certification Schemes Metaframework[1], the 2018 study "Certification schemes for Cloud Computing" prepared for the European Commission DG Communications Networks, Content & Technology, and the work performed by the Cloud Service Provider Certification Working group, created on December 2017, from April 2018 to June 2019 in response to the European Cybersecurity Act (EUCA), Title III, which aims to set the grounds to establish an EU-wide framework for cybersecurity certification of ICT services, products and processes, including those services provisioned by Cloud Service Providers (CSP).

Compliance with these security objectives can be established through the mapping of Cloud providers' security controls and practices into existing industry standards such as, for example, ISO 27000-based or equivalent standards.

In the scope of Mini-Competitions, Cloud providers are requested to document the control effectiveness assurance of their offer of Cloud Services using the **Effectiveness Assurance Levels (EAL's)** defined in section 3 of this Annex.

The answers of the providers will be used by the Participating Entities' technical services to determine the nature of systems that can be deployed at a specific provider, different risk profiles requiring different assurance levels.

## 2. Security Objectives

The list of **Security Objectives** relevant for the procedure is below:

| # | Security Objectives | Security Objectives Descriptions |
|---|---|---|
| SO-01 | **Information security policy** | Ensure the definition of policies related to information security, aligned with the relevant laws, regulations, as well as with the business requirements of the organization. It also includes the definition of the appropriate roles and responsibilities to carry out the implementation of said policies. |
| SO-02 | **Personnel and Training** | Ensure that the employees and contractors are aware and understand their responsibilities towards the information security policies defined and implemented in the organization. |
| SO-03 | **Asset management** | Provide mechanisms for the identification and protection of organizational and information assets, also those coming from customers. |
| SO-04 | **Identity and Access Management** | Put in place the mechanisms to ensure the access to the information, information processing facilities and virtualized environments of only authorized users. |
| SO-05 | **Cryptography and Key management** | Ensure a secure operation of the Cloud Services with the definition and implementation of the appropriate cryptographic mechanisms. |
| SO-06 | **Physical Infrastructure Security** | Ensure the prevention of unauthorized access to the physical site so as to prevent any damage, loss, failure or theft of any of the business' assets that may hamper the organization's operations of the Cloud Services. |

[1] v1.0, available from: https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-computing-certification

| # | Security Objectives | Security Objectives Descriptions |
|---|---|---|
| SO-07 | **Operational Security** | Ensure the secure and proper operation of the information security facilities so that the Cloud Services are always operational. |
| SO-08 | **Communications Security** | Ensure the protection of the information in networks, external and internal and in between systems. |
| SO-09 | **Procurement Management** | Define and implement mechanisms to manage the whole supply chain of the cloud service provider and ensure that these procurement activities maintain the appropriate security level. |
| SO-10 | **Incident Management** | Provide the means to manage, react to, and communicate security incidents. |
| SO-11 | **Business Continuity and Disaster Recovery** | Set out the activities needed to ensure the continuity of the operations of the cloud service recovery, including the disaster recovery ones while ensuring the integrity of the information at all times. |
| SO-12 | **Compliance** | Satisfy the legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. |
| SO-13 | **Security assessment** | To establish and maintain appropriate procedures for testing key network and information systems underpinning the Cloud Services and to establish and maintain appropriate procedures to perform security assessments of critical assets. |
| SO-14 | **Interoperability and Portability** | Provide means that allow customers to interface with other Cloud Services and/or if needed port to other providers offering similar services in a secure way |
| SO-15 | **System Security and Integrity** | Put in place the appropriate measures to ensure that the system maintains an adequate level of security and integrity in its entire lifecycle, from development to operation, from internal developments to outsourced ones, using both commercial and open source software. |
| SO-16 | **Change and Configuration Management** | Establish and maintain change management procedures for network and information systems. |
| SO-17 | **Risk management** | Provide the means to ensure an appropriate governance and risk management framework, as well as mechanisms to identify and address risks for the security of the Cloud Services. |
| SO-18 | **Security of Personal Data** | Put in place the appropriate measures and means so the provider give assurance to data controller that the provider fulfils its duties as data processor towards personal data protection. |

## 3. Effectiveness Assurance Levels

The detailed list of **Effectiveness Assurance Levels** relevant for the procedure is provided below:

| Effectiveness Assurance Levels (EAL's) | Descriptions |
|---|---|
| EAL-0 | There is no assurance that the security objective is met. Such an 'assurance level' essentially makes the affected security objective and security controls non-mandatory for evaluation. Cloud providers are nevertheless expected to exercise due care and follow best practices in their compliance with the security objective and implementation of the relevant security controls. |
| EAL-1 | The assurance that the security objective is met is provided by legally binding service description and contractual documents (including providers' responses to the procedure). |
| EAL-2 | The assurance that the security objective is met is provided by a self-assessment of the Cloud Services performed by Cloud providers, which must contain the list of implemented security controls. This is equivalent to 'CSA STAR 1: Self-Assessment' in the STAR (Security, Trust and Assurance Registry) Program of the CSA (Cloud Security Alliance). |
| EAL-3 | The assurance that the security objective is met is provided by audit reports of the Cloud Services delivered by Cloud providers' internal audit departments. |
| EAL-4 | The assurance that the security objective is met is provided by audit reports of the Cloud Services delivered by EU Member States or independent auditors (equivalent to 'CSA STAR 2: 3rd-party assessment-based certification'). |
| EAL-5 | The assurance that the security objective is met is provided by continuous monitoring-based certification of the Cloud Services, equivalent to 'CSA STAR 3'. |

The table refers to the methodology of the certification system of the Cloud Security Alliance (CSA). "*The CSA Security, Trust and Assurance Registry (STAR) program is a comprehensive set of offerings for cloud provider trust and assurance. The CSA STAR Program is a publicly accessible registry designed to recognize the varying assurance requirements and maturity levels of providers and consumers, and is used by customers, providers, industries and governments around the world. STAR consists of 3 levels of assurance, which currently cover 4 unique offerings. All offerings are based upon our succinct yet comprehensive list of cloud-centric control objectives in our Cloud Controls Matrix (CCM). CCM is the only meta-framework of cloud-specific security controls, mapped to leading standards, best practices and regulations*".

(source : https://cloudsecurityalliance.org/star/)

## 4. Demonstration of Security Objectives' Effectiveness

The Contracting Authority will assess, for **each Security Objective** defined in section 2, the **Effectiveness Assurance Levels (EALs)** of the Cloud Services of the provider. The Contracting Authority will proceed as follows to establish this EAL:

- The Contracting Authority will request a **self-assessment of the EALs** of the Cloud Services by the provider, for each security objective.

- The Contracting Authority considers that the provider can justify its self-assessment of the EAL by:

  - Providing the **means** through which the security objective is implemented (i.e. certification, respect of standards or internal processes)
  - Providing the **list of services** for which the security objective is implemented (i.e. list of services certified or following an internal process)

  Therefore the Contracting Authority will ask the providers:

  - **Certifications** obtained and relevant for security objective (this justification will provide the best marks in case of evaluation of the offer)
  - Or, **Internal documentation** justifying implementation of **security practices**
  - Or, **Internal documentation** justifying implementation of a **standard**

  To verify the reality of the certifications, the Contracting Authority will request a sample of the audit certificates, attestations and scope of applicability of the certifification. The Contracting Authority may also request a specific certification, attestation and scope of applicability for a specific service at any time during the execution of the Contract.

For reference, the Contracting Authority provides a table of coverage of the security objectives towards industry certifications. Therefore providers able to produce evidence for certification will only have to refer to the applicable certification and will not have to produce further documents. The table published in the DPS is provided below.

For each Mini-Competition, minimum EALs, i.e. level of security of the Cloud Services offered, will be required by the Contracting Authority depending on the needs of the customer of the Cloud Services. It is reminded to Participants of the DPS that the Participating Entities are in general expecting a high level of security of their suppliers, and therefore high effective assurance levels.

| | 1. Information security policy | 2. Personnel & Training | 3. Asset Managenent | 4. Identity and access management | 5. Cryptography and Key management | 6. Physical Infrastructure Security | 7. Operational Security | 8. Communications Security | 9. Procurement Management | 10. Incident Management | 11. Business Continuity and DRP | 12. Compliance | 13. Security Assessment | 14. Interoperability and Portability | 15. System Security and Integrity | 16. Change & Configuration Management | 17. Risk Management | 18. Security of Personal Data |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SecNumC oud | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟨 |
| BSI C5 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟨 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟨 | 🟩 | 🟩 | 🟥 | 🟩 | 🟥 | 🟨 |
| ISO/IEC 27002 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟥 | 🟩 | 🟨 | 🟨 |
| ISO/IEC 27017 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟥 | 🟩 | 🟨 | 🟨 |
| ISO/IEC 27018 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟨 | 🟨 | 🟩 | 🟨 | ⬜ |
| CSA CCM | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟨 |
| CSA OCF a:tes'at on 1 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟨 |
| CSA OCF attes ation 2 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟨 |
| CSA OCF certifica ion 2 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟨 |
| AICPA SCC1 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 |
| SOC2 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟨 |
| SOC3 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟨 |
| Eurocloud self-assessment | 🟩 | 🟥 | 🟥 | 🟨 | 🟥 | 🟥 | 🟨 | 🟨 | 🟥 | 🟩 | 🟨 | 🟩 | 🟩 | 🟥 | 🟥 | 🟨 | 🟨 | 🟨 |
| Eurocloud star audit | 🟩 | 🟥 | 🟥 | 🟨 | 🟥 | 🟥 | 🟨 | 🟨 | 🟥 | 🟩 | 🟨 | 🟩 | 🟩 | 🟥 | 🟥 | 🟨 | 🟨 | 🟨 |
| PCI | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 |
| Leet Security | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟨 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟨 | 🟩 | 🟩 | 🟨 |
| NIST 800 - 53 | 🟩 | 🟩 | 🟥 | 🟥 | 🟩 | 🟩 | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟩 | 🟥 | 🟥 | 🟩 | 🟩 | 🟩 | 🟨 |
| Certified cloud service TüV | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟨 | 🟩 | 🟩 | 🟨 | 🟩 | 🟥 | 🟩 | 🟩 | 🟩 | 🟨 |
| ISO 17203 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 |
| ISO 17789 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 |
| ISO 19944 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 |
| ISO 19941 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟩 | 🟥 | 🟥 | 🟥 | 🟨 |
| ISO 19086 | 🟩 | 🟩 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 | 🟨 | 🟨 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 |
| ISO 19099 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 |
| ISO 22301 | 🟩 | 🟨 | 🟥 | 🟩 | 🟥 | 🟥 | 🟨 | 🟥 | 🟥 | 🟩 | 🟩 | 🟨 | 🟨 | 🟥 | 🟥 | ⬜ | 🟨 | 🟨 |
| ISO/IEC 24760 | 🟨 | 🟨 | 🟥 | 🟩 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 | 🟨 |
| ISOIEC 29100 | 🟨 | 🟨 | 🟥 | 🟩 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 | 🟨 |
| ISO/IEC 29101 | 🟨 | 🟨 | 🟥 | 🟩 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 | 🟨 |
| ISO/IEC 29115 | 🟨 | 🟨 | 🟥 | 🟥 | 🟥 | 🟨 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 | 🟨 |
| SAML | 🟥 | 🟥 | 🟥 | 🟨 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 |
| OAuth2.0 | 🟥 | 🟥 | 🟥 | 🟨 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 |
| OpenID | 🟥 | 🟥 | 🟥 | 🟨 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟥 | 🟨 |

| | |
|---|---|
| 🟩 | Fully |
| 🟨 | Partially |
| 🟥 | Not covered |