Cloud Financial Services. October 2015

An Overview of CAIXABANK– Introduction

CaixaBank is the leading financial group in Spain, both in banking and insurance and it is developing a strategy of diversification with stakes in international banks and also within leading service companies.

14.1M Customers

32K Employees
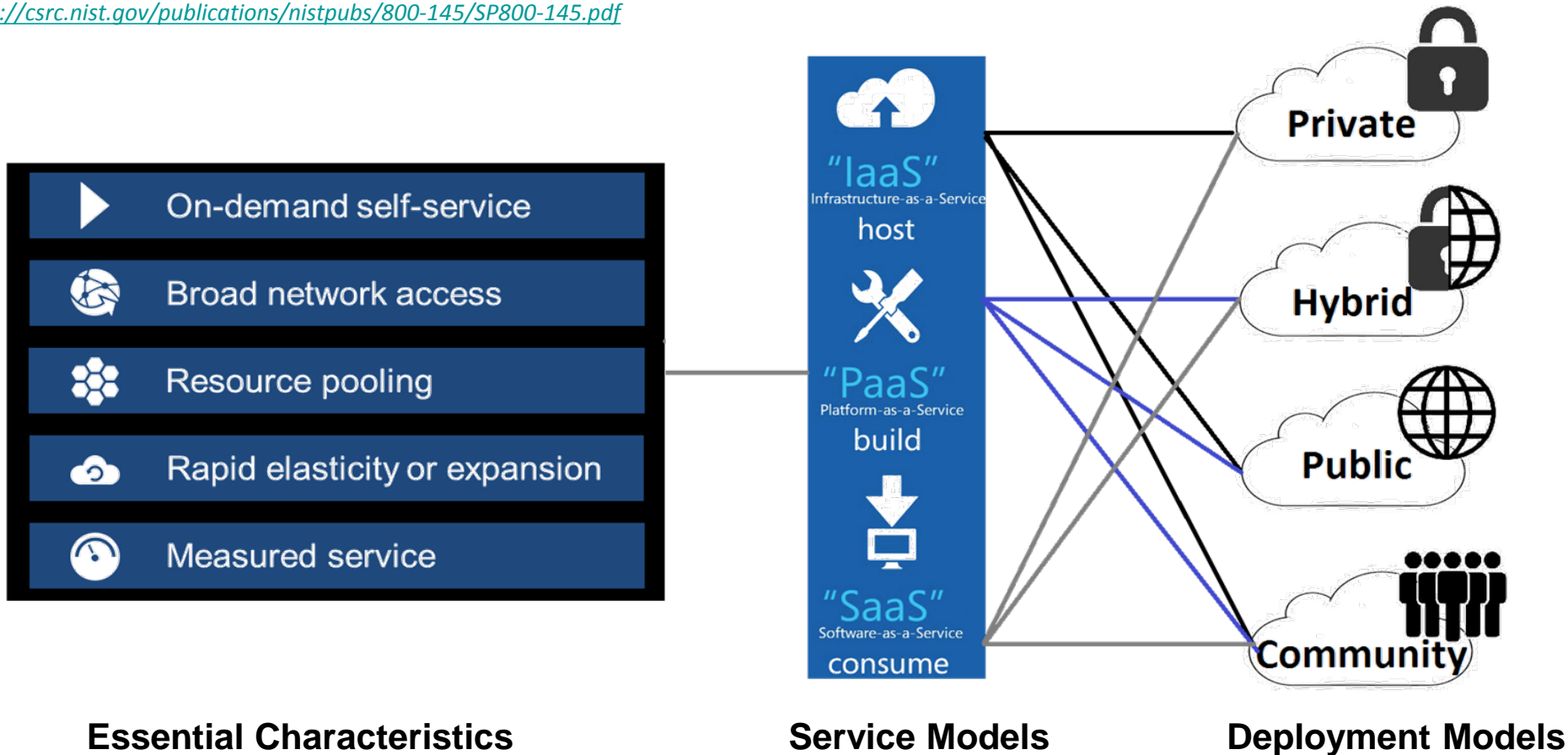
6K Branches

10K ATMs

CaixaBank is currently chairing The Financial Services Working Group (FSWG), within the Cloud Security Alliance (CSA), was created and officially presented at the 2014 CSA EMEA Congress. The FSWG **emerged to provide knowledge and guidance on how secure cloud solutions can be delivered and managed by the financial industry.**

cloud security alliance®

The NIST Definition of Cloud Computing

*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, **three service models, and four deployment models.***

http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Essential Characteristics

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity or expansion
- Measured service

Service Models

"IaaS"
Infrastructure-as-a-Service
host

"PaaS"
Platform-as-a-Service
build

"SaaS"
Software-as-a-Service
consume

Deployment Models

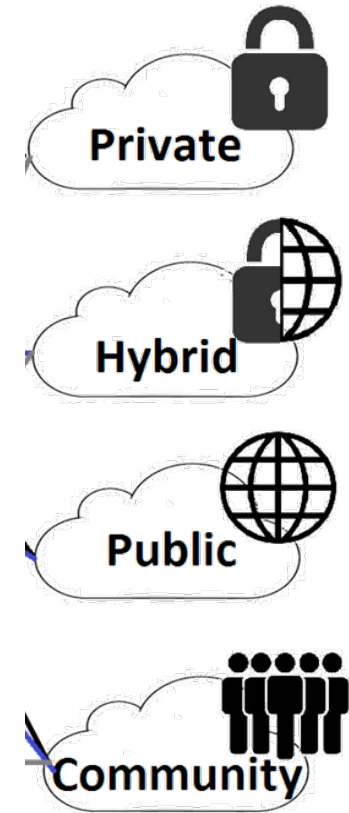Private

Hybrid

Public

Community

3

ISO/IEC 17788 – Cloud Computing – Overview and Vocabulary

Cloud computing is a paradigm for enabling network access to a scalable and elastic pool of shareable physical o virtual resources with on-demand self-service provisioning and administration.

- ▶ On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity or expansion
- Measured service
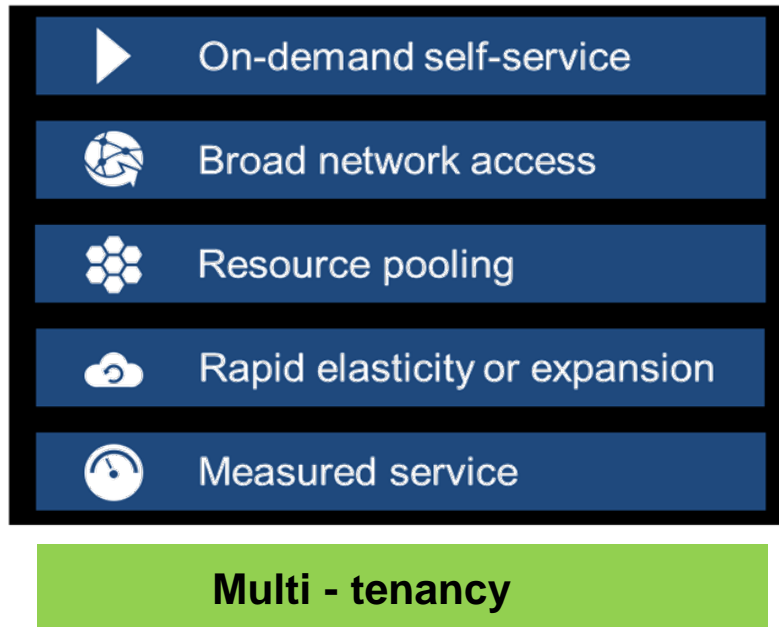
Multi - tenancy

NIST Service Models substituted by an infinite number of "Guff-as-a-service"

Private

Hybrid

Public

Community

Key Characteristics

~~Service Models~~

Deployment Models

* Multi-tenancy is a feature where physical or virtual resources are allocated in such a way that multiple tenants and their computations and data are isolated from and inaccessible to one another.

ISO/IEC 17788 – Cloud Computing – Overview and Vocabulary

Three Service Models (types) were redefined as "**Cloud Service categories**" and new categories were added. Types introduced as "**Cloud Capabilities Types**".

Cloud Service Categories	Cloud Capabilities Types		
	Infrastructure	Platform	Application
Software as a Service			✓
Platform as a Service		✓	
Infrastructure as a Service	✓		
Network as a Service	✓	✓	✓
Data Storage as a Service	✓	✓	✓
Compute as a Service	✓		
Communication as a Service		✓	✓

CaixaBank

CaixaBank Cloud Computing – State of Art

NO CLOUD strategy

YES SECURE CLOUD strategy

2012

2015

Restrictive Security Guideline for Cloud Computing defined

New strategy for cloud computing

Security Guideline for Cloud Computing

| Risks identification | Security Strategy | Security Controls definition |

Cloud Service lifecycle in CaixaBank:

- Cloud Service need
- CSP evaluation
- Cloud Service acquisition
- Review and Monitoring
- Cloud Service Audit

enisa

CLOUD CERTIFICATION SCHEMES LIST

Cloud Certification Schemes List

Guideline Go/ NO Go to cloud

ISO/IEC 19086 (SLA framework)

Cloud Security Measures in contracts

Cloud Control Matrix

CSP audit

cloud security alliance®

CSA

Cloud Financial Services. October 2015
16280 – Security / Control Service

6

The Security Guideline for Cloud Computing

Security Guideline for Cloud Computing

Risks identification	**Security Strategy**	Security Controls definition
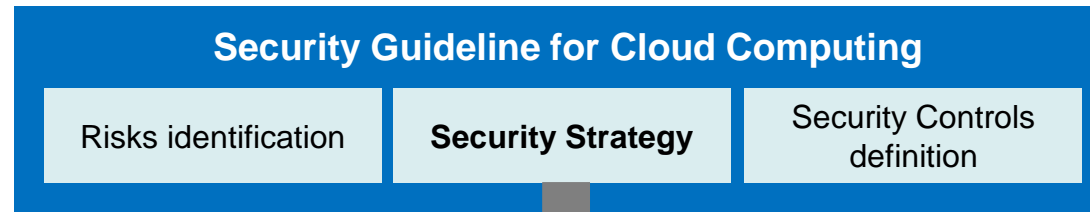
In the case of contracting cloud services to CSP, apply each and every one of the security measures set out in the Security Regulatory Body od CaixaBank shall be applied.

Specific measures shall be considered for:
- Personal Data Protection (compliance with Spanish Personal Data Protection law)
- Credit card data protection (compliance with PCI DSS).
- Administration and authentication of users and administrators
- Using cryptography (communications and data storage)
- Contracts with CSP
- Internal Audit (by CSP), External audit (by CaixaBank)

Very restrictive guideline inhibiting the acquisition of Cloud Services

➡

Acquisition of cloud services without involving security department.

Cloud Financial Services. October 2015
16280 – Security / Control Service

7

Cloud Computing Threats and Risks – actual analysis

2015

The Notorious Nine (Cloud Computing Top Threats in 2013)	Scope	Risk
Data Breaches	**Confidentiality**	Information Leakage
Data Loos		Sensitive information accessible by the Cloud Service Provider (CSP)
Account or Service Traffic Hijacking		Safe disposal after retention period
Insecure Interfaces and APIs	**Service Control**	Lost of administration control
Denial of Service	**Traceability & Auditability**	Availability and correct managements of evidences.
Malicious Insider	**Shared Environments**	Security issues affecting other Cloud customers may impact the environment of CaixaBank
Abuse of Cloud Services	**Business Continuity**	Inability to scale the service
Insufficient Due Diligence		Limitations on interoperability with other platforms
Shared Technology Vulnerabilities		Possibility of increased risk of SPoF (simple point of fault)
	Service Termination	Elimination of information after service termination
		Complex and costly migration or finishing processes
	Legal Requirements	Gaps in identification of legal compliance impacts

cloud security alliance®

Top Threats Working Group

https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

Contracting Cloud Service Provider - Security Measures

2015

Security Clauses in the Contract with Cloud Service Provider (CSP):

1) Information treatment
2) Compliance with internal regulations
3) Compliance with national and international laws and regulations
4) Business Continuity
5) Security incident reporting
6) Scalability
7) Auditability
8) Interoperability
9) Termination of service
10) Maintaining security certification fulfilled by CSP during the period of the contract validity

Cloud Service Oriented certifications:

- CSA STAR
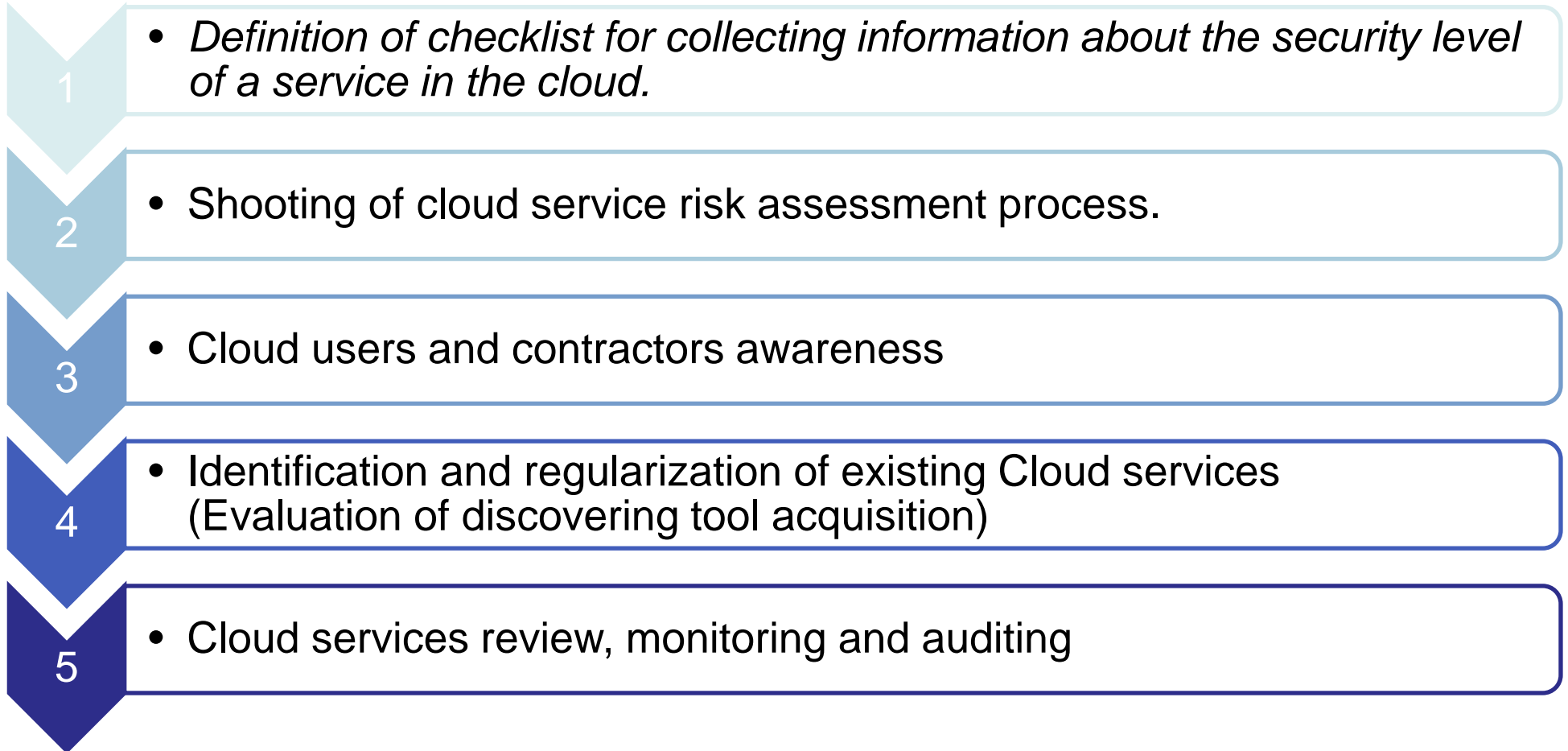- ISO/IEC FDIS 270017 (under development)

Certifications that can help to establish CSP security level:

- SSAE 16
- PCI DSS v.3
- ISO/IEC 27001:2013

During **evaluations of CSP security level** will be:
a) Verified that certification scope covers the scope of contracted service.
b) Verified that CSP was audited by independent and qualified third party.
c) Considered the maturity of implemented controls.

Future Steps in Cloud Computing

1 • *Definition of checklist for collecting information about the security level of a service in the cloud.*

2 • Shooting of cloud service risk assessment process.

3 • Cloud users and contractors awareness

4 • Identification and regularization of existing Cloud services (Evaluation of discovering tool acquisition)

5 • Cloud services review, monitoring and auditing

Cloud Financial Services – Thanks!!

THANK YOU!!!

Questions??

Mario Maawad Marcos

Director of Fraud Prevention / Security & Service Control
Co-Chair of the Financial Services Working Group at Cloud Security Alliance

mmaawad@caixabank.com