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.

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.
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.

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

**Key Characteristics**

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

**NIST Service Models**

- Private
- Hybrid
- Public
- Community

Substituted by an infinite number of “Guff-as-a-service”

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

<table>
<thead>
<tr>
<th>Cloud Service Categories</th>
<th>Cloud Capabilities Types</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Infrastructure</td>
</tr>
<tr>
<td>Software as a Service</td>
<td></td>
</tr>
<tr>
<td>Platform as a Service</td>
<td></td>
</tr>
<tr>
<td>Infrastructure as a Service</td>
<td>✓</td>
</tr>
<tr>
<td>Network as a Service</td>
<td>✓</td>
</tr>
<tr>
<td>Data Storage as a Service</td>
<td>✓</td>
</tr>
<tr>
<td>Compute as a Service</td>
<td>✓</td>
</tr>
<tr>
<td>Communication as a Service</td>
<td></td>
</tr>
</tbody>
</table>
CaixaBank Cloud Computing – State of Art

NO CLOUD strategy

2012

Restrictive Security Guideline for Cloud Computing defined

2015

YES SECURE CLOUD strategy

New strategy for cloud computing

Cloud Service lifecycle in CaixaBank:

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

Security Guideline for Cloud Computing

- Risks identification
- Security Strategy
- Security Controls definition

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

enisa

cloud security alliance®
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 of 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)
### Cloud Computing Threats and Risks – actual analysis

#### The Notorious Nine

(Cloud Computing Top Threats in 2013)

<table>
<thead>
<tr>
<th>Threat</th>
<th>Scope</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Breaches</td>
<td>Confidentiality</td>
<td>Information Leakage</td>
</tr>
<tr>
<td>Data Loos</td>
<td>Service Control</td>
<td>Sensitive information accessible by the Cloud Service Provider (CSP)</td>
</tr>
<tr>
<td>Account or Service Traffic Hijacking</td>
<td>Traceability &amp; Auditability</td>
<td>Safe disposal after retention period</td>
</tr>
<tr>
<td>Insecure Interfaces and APIs</td>
<td>Shared Environments</td>
<td>Lost of administration control</td>
</tr>
<tr>
<td>Denial of Service</td>
<td></td>
<td>Availability and correct managements of evidences.</td>
</tr>
<tr>
<td>Malicious Insider</td>
<td></td>
<td>Security issues affecting other Cloud customers may impact the environment of CaixaBank</td>
</tr>
<tr>
<td>Abuse of Cloud Services</td>
<td></td>
<td>Inability to scale the service</td>
</tr>
<tr>
<td>Insufficient Due Diligence</td>
<td></td>
<td>Limitations on interoperability with other platforms</td>
</tr>
<tr>
<td>Shared Technology Vulnerabilities</td>
<td></td>
<td>Possibility of increased risk of SPoF (simple point of fault)</td>
</tr>
</tbody>
</table>

#### Top Threats Working Group

Contracting Cloud Service Provider - Security Measures

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
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