AWS for Finance Institutes

The 1st Steps to adopt AWS

Bertram Dorn
Specialized Solutions Architect for Security and Compliance

30. Juni 2016
Infrastructure
What is DevOps?

**Software development lifecycle**

- **delivery pipeline**
  - build
  - test
  - release

- **feedback loop**
  - plan
  - monitor

**DevOps** = efficiencies that speed up this lifecycle
Monolith development lifecycle

developers

app

delivery pipeline

build
test
release
Microservice development lifecycle

developers — services — delivery pipelines

- build
- test
- release
Service-Oriented Architecture (SOA)

Single-purpose

Connected through APIs

Highly decoupled

“Microservices”
Dedicated Security Services

- Tenant Isolation
- Deep Network Security
- Scaling Crypto Services
- Detailed Monitoring
- Access Control
  - Mandatory
  - Fine Grade
  - MFA Possible
Security Possibilities

**Lift and Shift**
- Integrate standards
- Replicate

**Transparency**
- Monitor Every Activity

**Scale and Innovate**
- Use Cloud Security
  - Continuous Security
  - Permanent Monitoring/Audit
    - Automatic Reaction
    - Permanent Monitoring
    - Integrated Audit
    - Security - DevOps
Report of Independent Accountants

To the Board of Directors of Amazon Web Services, Inc.

We have examined management’s assertion that Amazon Web Services, Inc. (AWS), during the period October 1, 2015 through March 31, 2016, maintained effective controls to provide reasonable assurance that:

- the Amazon Web Services System was protected against unauthorized access, use, or modification to meet AWS’ commitments and system requirements
- the Amazon Web Services System was available for operation and use to meet AWS’ commitments and system requirements

based on the criteria for security and availability in the American Institute of Certified Public Accountants’ TSP section 100, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy updated as of March 2016. This assertion is the responsibility of AWS management. Our responsibility is to express an opinion based on our examination.
Point-in-time, or continuous compliance assessments?
Shared Responsibility

Optimized Network/OS/App Controls
Service-specific Controls
Cross-service Controls
Cloud Service Provider Controls

Managed by Customer
Managed by AWS

Security in the Cloud
Security of the Cloud

Request reports at: aws.amazon.com/compliance/#contact

ISO 27000
ISO 9001

AICPA SOC
FedRAMP
FedRAMP FIPS
HIPAA
FISMA
ITAR
The main AWS Compliance Frameworks of today

<table>
<thead>
<tr>
<th>Certificates:</th>
<th>Programmes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 27000</td>
<td>PCI DSS Level 1</td>
</tr>
<tr>
<td>AICPA SOC</td>
<td>SOC 1/ ISAE 3402</td>
</tr>
<tr>
<td>ISO 9001</td>
<td>SOC 2</td>
</tr>
<tr>
<td>ITAR</td>
<td>SOC 3</td>
</tr>
<tr>
<td>FIPS</td>
<td>ISO 9001</td>
</tr>
<tr>
<td>MPAA</td>
<td>IRAP (Australia)</td>
</tr>
<tr>
<td>FIPS 140-2</td>
<td>FIPS 140-2</td>
</tr>
<tr>
<td>ISO 9001</td>
<td>FIPS 140-2</td>
</tr>
<tr>
<td>MPAA</td>
<td>CJIS</td>
</tr>
<tr>
<td>FISMA</td>
<td>CSA</td>
</tr>
<tr>
<td>ISA 3402</td>
<td>FERPA</td>
</tr>
<tr>
<td>HIPAA</td>
<td>MPAA</td>
</tr>
<tr>
<td>FedRAMP (SM)</td>
<td>G-Cloud</td>
</tr>
<tr>
<td>DoD CSM Levels 1-2, 3-5</td>
<td>MTCS Tier 3 Certification</td>
</tr>
<tr>
<td>DIACAP and FISMA</td>
<td>ITAR</td>
</tr>
<tr>
<td>ISO 27001</td>
<td>Section 508 / VPAT</td>
</tr>
</tbody>
</table>
Scope

- By Service (not only Datacenter)
- By Region
- By Certification
- Global
- Scalable
Auftragsdatenvereinbarung
Inclusive
Technische und Organisatorische Massnahmen
Compliance Requirements

Mapping of Internal Controls → AWS Control Framework
Mapping of Regulator Controls → AWS Control Framework
Meeting Regulator/Legal Requirements → Enterprise Agreement
Continuous Monitoring → EA + AWS Controls

- Discuss the Needs in the Enterprise Agreement
- Dive Deep in the AWS Control Framework
- Learn and Integrate the AWS Security Technology
Vielen Dank

Bertram Dorn
What is AWS?

- AWS Global Infrastructure
- Networking
- Database
- Storage
- Compute
- Application Services
- Deployment & Administration
An independent collection of AWS resources in a defined geography

A solid foundation for meeting location-dependent privacy and compliance requirements\(^\text{1}\)
Availability Zone

Designed as independent failure zones

Physically separated within a typical metropolitan region