Auslagerung in die Cloud: Viele Wege - ein Ziel

Gerald Boyne
Head of Security Assurance DACH

AGENDA

- Erfolgsfaktoren
  für agile Produktentwicklung im Zuge der Digitalisierung

- Wie lassen sich
  agile Digital-Produkte systematisch kontrollieren

- Wie erhält man seine Betriebsstabilität
  und Compliance in der Cloud

amazon web services

ERFOLGSFAKTOREN FÜR AGILE PRODUKTENTWICKLUNG IM ZUGE DER DIGITALISIERUNG

Why Are Fin Serv Companies Adopting Cloud Computing?

Regulatory Compliance Continues to Drive Expense

Security, **Compliance**, and **Reduced Cost**

A Desire For Increased Wallet Share is Driving a Focus on Innovation

Ability to Bring **New Ideas** to Market ***Faster***

Increasing Amounts of Data, Finite Resources for Analytics

Highly Scalable Infrastructure for **Analytics** that Matter to the Industry

---

Digitization and Disruptive Technology are Accelerating Transformation

Ability to **Transform** the **Enterprise** & the **Industry**

amazon web services

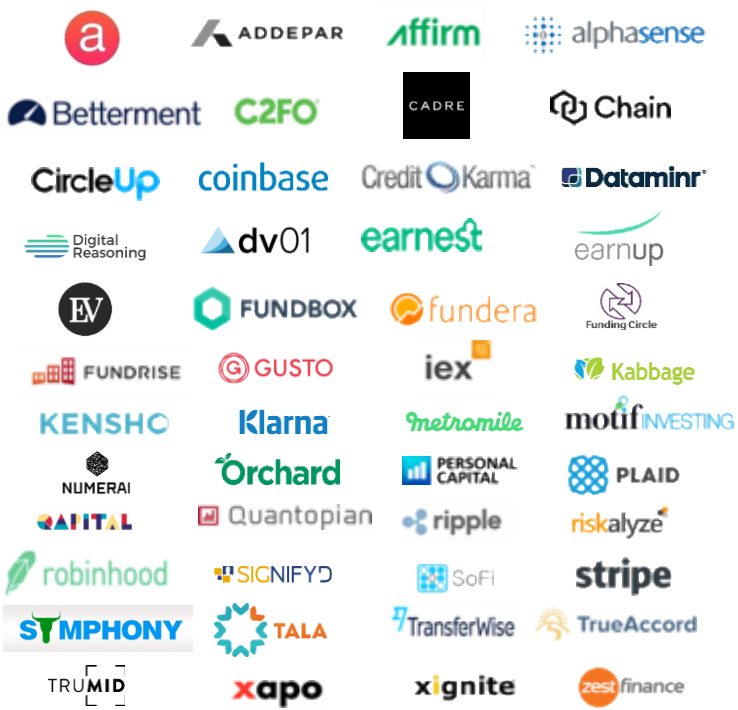
FinTech startups have also found a home on AWS

Percentage of the 2016 **Forbes FinTech 50** that use AWS

96%

"Banks aren't being disrupted by FinTech technology, they're being disrupted by customer expectations."

- McKinsey & Company



amazon web services

AWS in Banking & Payments

Suncorp is a diversified Australian financial services company with 14 brands and 4 lines of business in 5 countries. By choosing AWS to support Agile principles and practices, **Suncorp was able to launch a working virtual private cloud and virtual data center in under three months and plans to move 2,000 applications to AWS.**

5th Largest Bank in Australia

This G-SIB permits AWS to identify it as a customer, but not to disclose details related to its use cases.

G-SIB

[Withheld]

This G-SIB recently began migrating its **mission-critical high-performance computing (HPC) grids** to AWS, with 11 currently in production.

G-SIB

N26, a German **mobile-first bank**, **runs completely on AWS**. One of the hottest startups in Europe, N26 currently counts 300,000 bank accounts in 16 European countries and in the US , and **in July 2016 received banking licenses from the European Central Bank and BaFIN**.

Mobile-First Bank (Europe)

Mondo built a **cloud-native**, **mobile-first digital bank,** and received its UK bank license from the UK's FCA and PRA in August 2016. Mondo uses AWS to host its applications, including **core banking systems.**

UK Challenger Bank

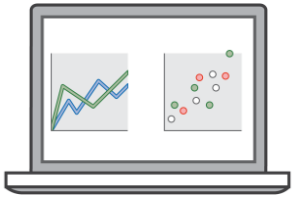
Simple **uses AWS to run its virtual banking platfor**m and meet payment card industry (PCI) data security standard (DSS) compliance for its development and production environments.

US Online Bank

Financial institutions trust AWS to transform their businesses

Banking & Payments

BBVA
DBS
monzo
STARLING BANK
OakNorth Bank
bankinter.
HOLVI
Capital One
iZettle®



Capital Markets

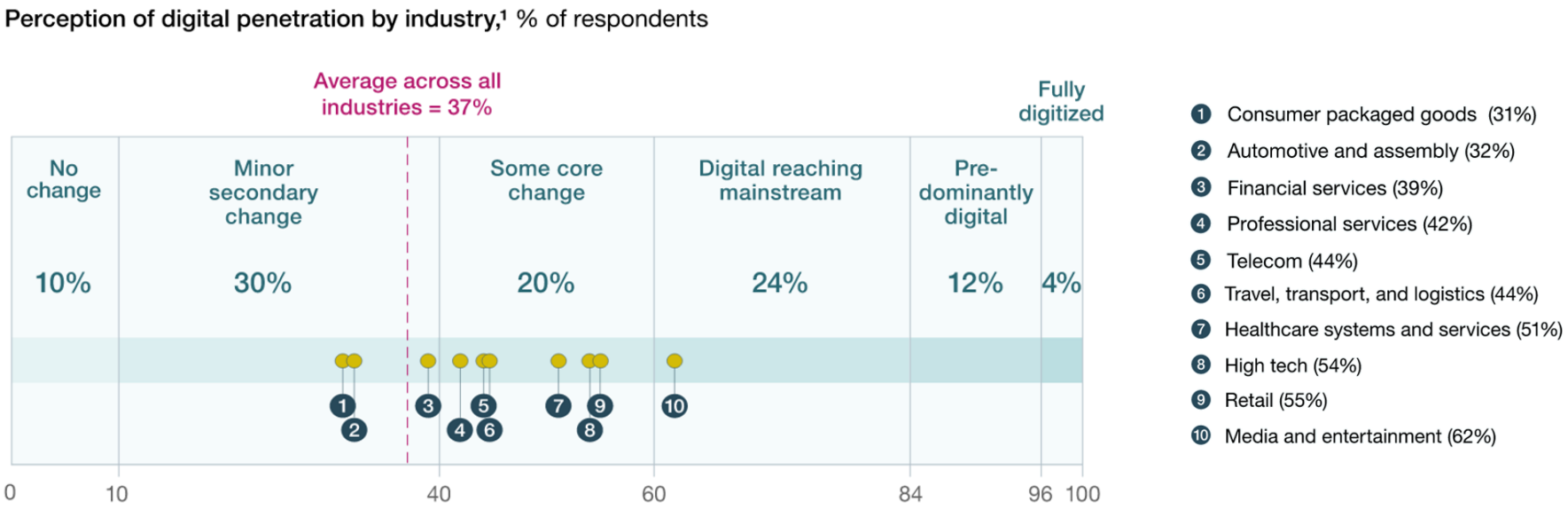
FINRA
London Stock Exchange
ISE
Nasdaq
robinhood
TRADING TECHNOLOGIES
Broadridge
MIRAE ASSET Global Investments
NATIONAL BANK

Insurance

mutuelle smatis PRÉVOYANCE
AON
MAPFRE
PACIFIC LIFE
Allianz
GUARDIAN
RADIAN
Liberty Mutual.

amazon web services

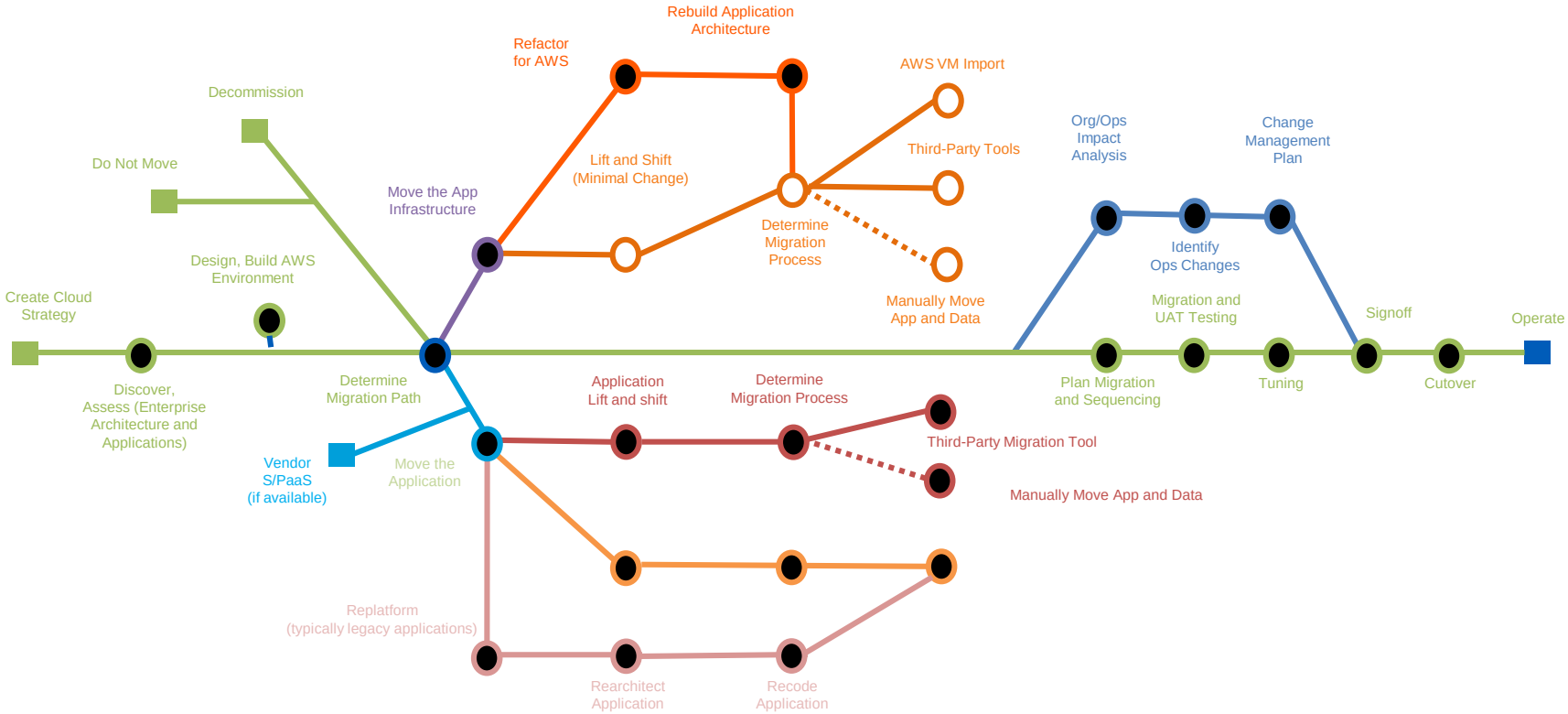
…to drive digital transformation



Source: McKinsey February 2017; survey of 310 financial services firms and 1200+ firms in other industries

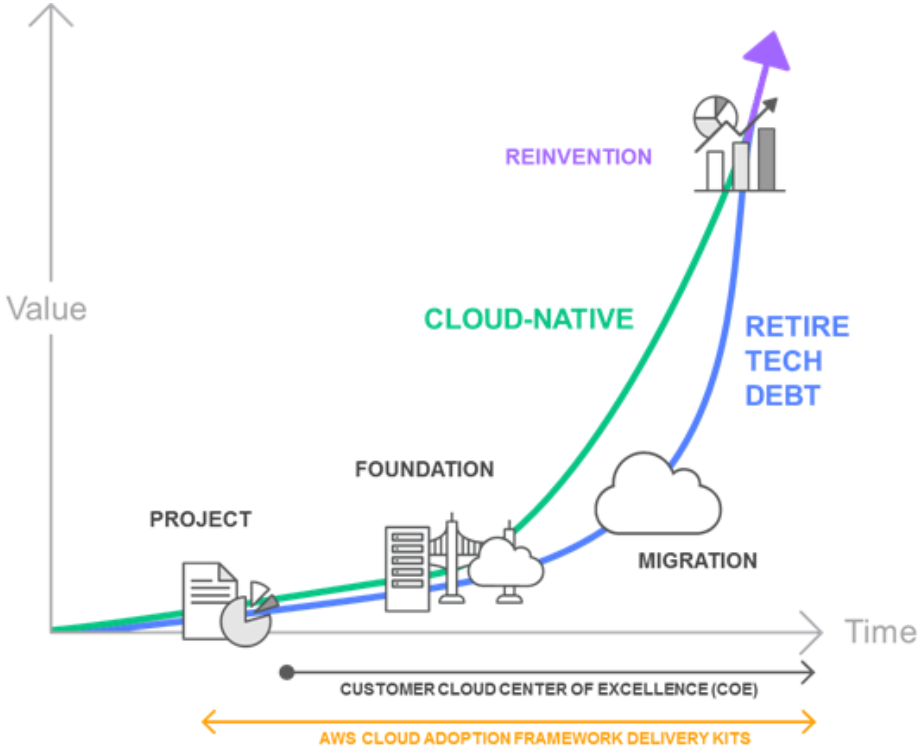
amazon web services

Many Paths To The Cloud – All Require Structure



amazon web services

Use the real value of the cloud



amazon web services

Process Example: Workload Migration Process

1-Develop

- Customers need to create their baseline AWS security controls for the enterprise
- Templates can be used for all accounts, roles, services and even customer applications

2-Define

- Determine what applications they want to move & current the legacy controls
- Further understand what requirements apply to the data, resiliency needs, & reporting

3-Modify

- Once the application is defined, baseline controls can be modified where appropriate
- Additional new controls can be implemented to meet individual application needs

4-Implement

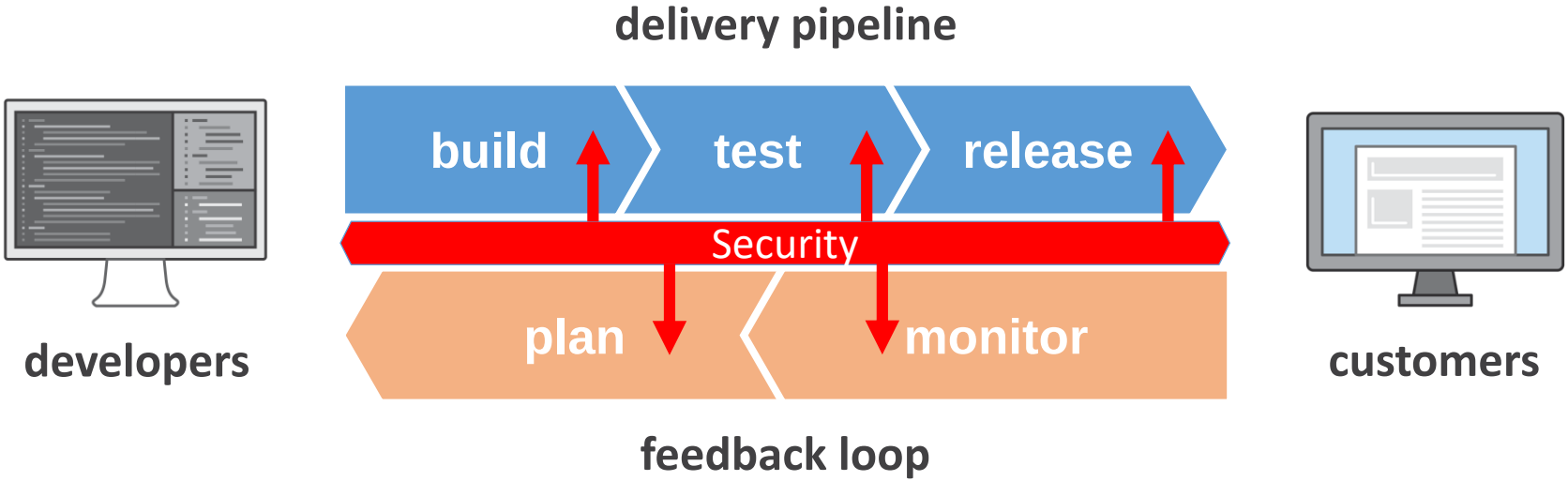
- Customers rollout the application specific controls in a test environment to validate
- The production environment is then configured and the application deployed

5-Monitor

- Automated monitoring & reporting is enabled to track performance, access & changes
- Monitoring results are reported to testing & auditing teams for continuous review

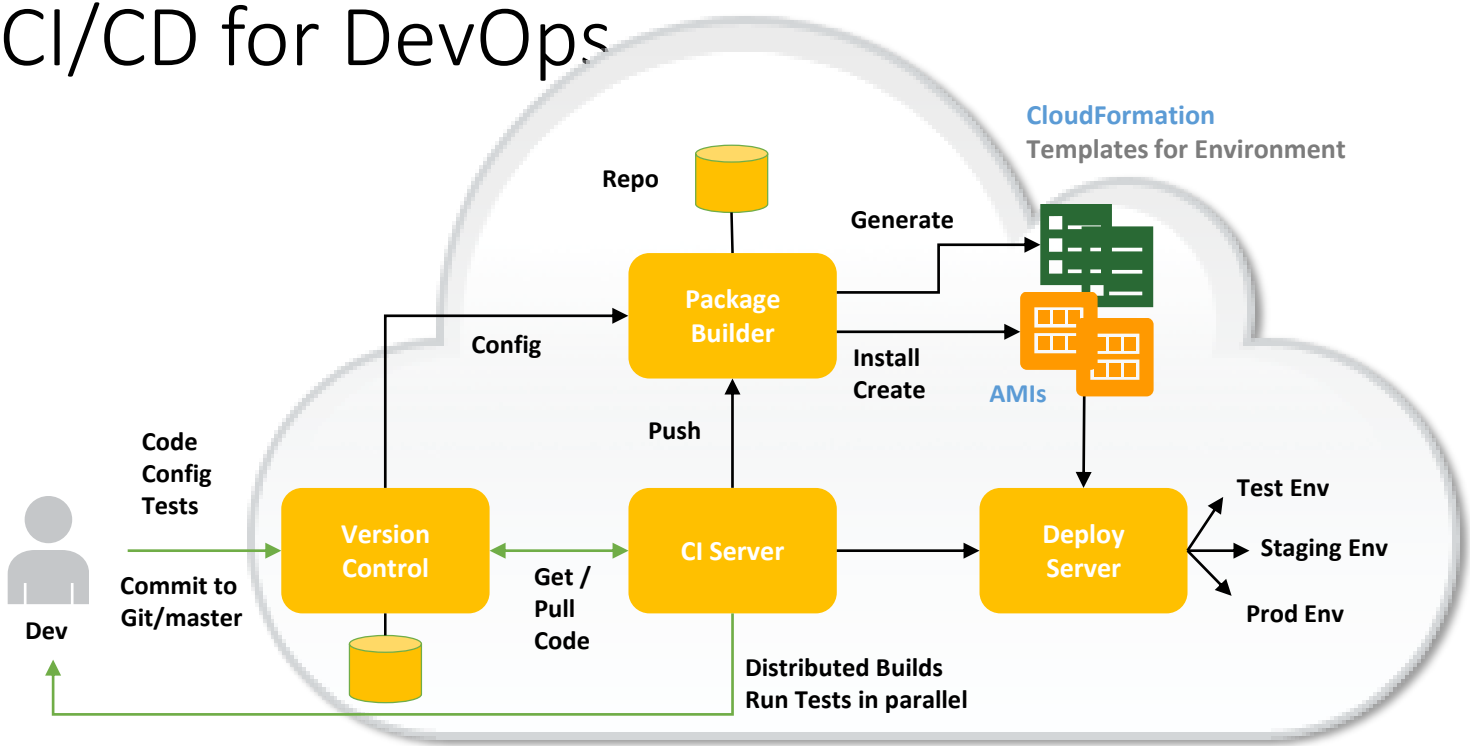
What is DevSecOps

Software development lifecycle



DevOps = Efficiencies that speed up this lifecycle
DevSecOps = Validate building blocks without slowing lifecycle

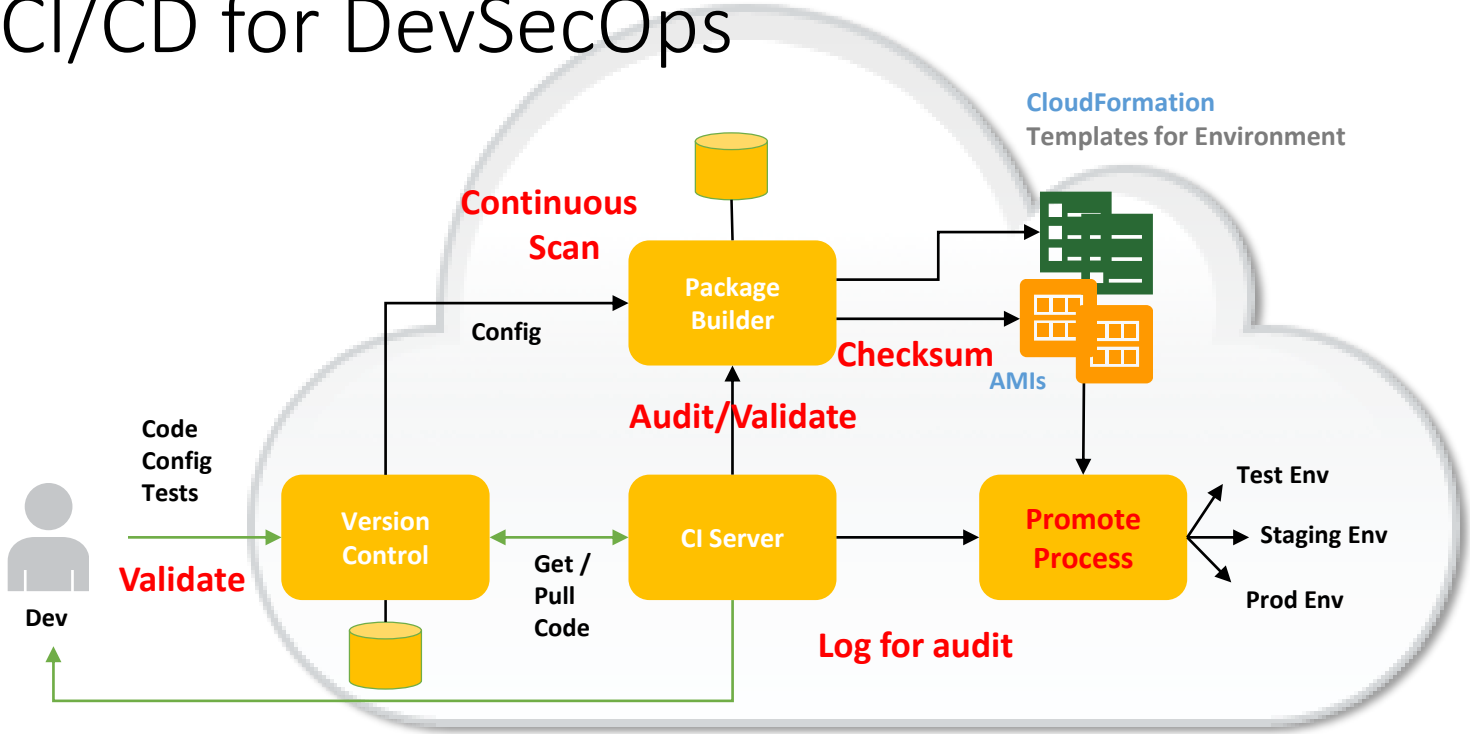
CI/CD for DevOps



Send Build Report to Dev

Stop everything if build failed

CI/CD for DevSecOps



Send Build Report to Security
Stop everything if audit/validation failed

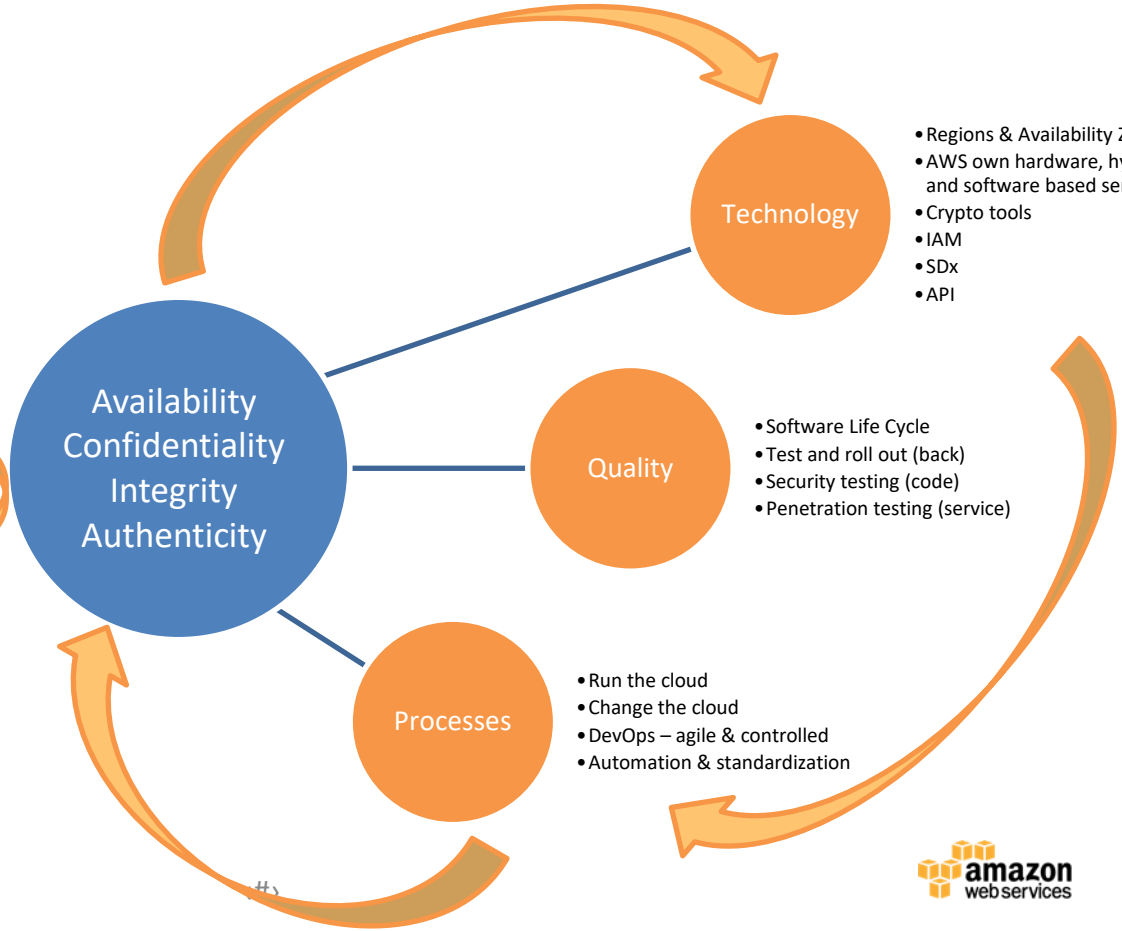
WIE LASSEN SICH AGILE DIGITAL-PRODUKTE SYSTEMATISCH KONTROLLIEREN

AWS Compliance Program Risk Landscape

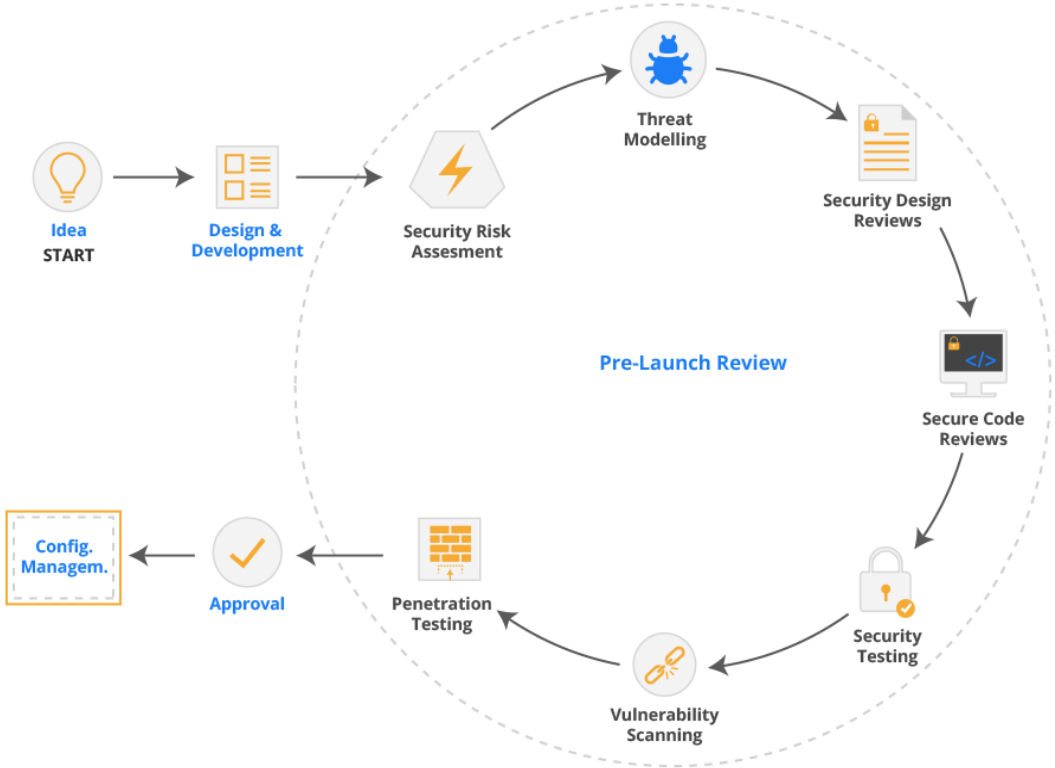
AWS is responsible for the product „cloud“

The product defines ACIA

ACIA designes the product



Service Pre-Launch Lifecycle



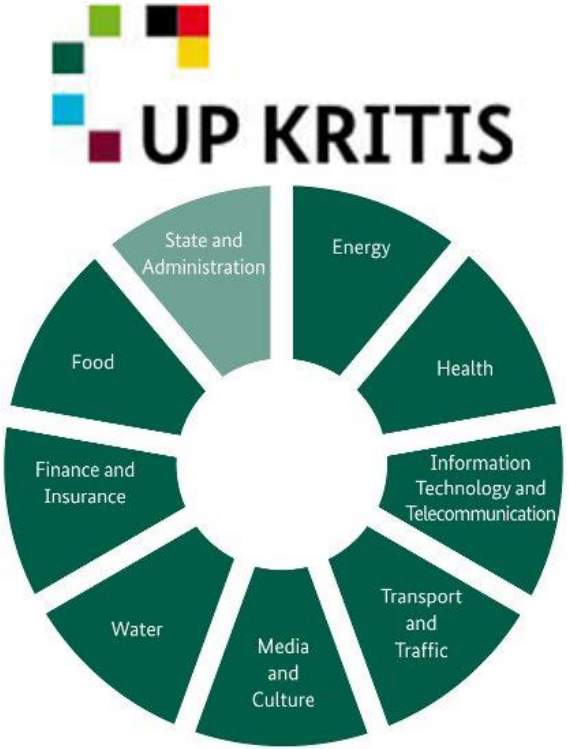
The main AWS Compliance Frameworks of today

Certificates:

Zertifizierungen/Testierungen	Gesetze, Vorschriften und Datenschutz	Harmonisierungen/Frameworks
C5 [Deutschland]	CISPE	CIS
Cyber Essentials Plus [UK]	Klauseln des EU-Modells	CJIS
DoD SRG	FERPA	CSA
FedRAMP	GLBA	ENS [Spanien]
FIPS	HIPAA	EU-US Privacy Shield
IRAP [Australien]	HITECH	FISC
ISO 9001	IRS 1075	FISMA
ISO 27001	ITAR	G-Cloud [GB]
ISO 27017	My Number Act [Japan]	GxP (FDA CFR 21 Part 11)
ISO 27018	U.K. DPA – 1988	ICREA
MLPS Level 3 [China]	VPAT / Section 508	IT-Grundschutz [Deutschland]
MTCS [Singapur]	EU-Datenschutzrichtlinie	MITA 3.0
PCI DSS Level 1	Privacy Act [Australien]	MPAA
SEC Rule 17-a-4(f)	Privacy Act [Neuseeland]	NIST
SOC 1	PDPA – 2010 [Malaysia]	PHR
SOC 2	PDPA – 2012 [Singapur]	Uptime Institute-Stufen
SOC 3	PIPEDA (Kanada)	Grundsätze der Cloud-Sicherheit von UK
	Spanische DPA-Autorisierung	

amazon web services

UPKRITIS – NIS-D



Network Information Security Directive

German Implementation Project for Critical Infrastructure

Based on the Information security Law of Germany (IT-Sig) of the German Office for information Security in Technology (BSI) https://www.bsi.bund.de/EN/TheBSI/BSIAct/bsiact_node.html - BSI developed together with the critical sector providers sector specific standards.

https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/UP%20KRITIS.pdf For data center housing and hosting (unequal of the cloud) a sector standard had been developed aligned with the ISO2001 certification in a scoped mode, focusing on operating a data center under an ISMS.

https://www.kritis.bund.de/SubSites/Kritis/EN/activities/national/cipimplementationplan/cipimplementationplan_node.html
This activity is named UPKRITIS for implementing project for critical infrastructure.

amazon web services

AWS Compliance Program Technology / products

Amazon Virtual Private Cloud (VPC)
Logically isolated section of the AWS cloud where you launch AWS resources in a virtual network that you define

AWS Organizations
Policy-based management for multiple AWS accounts

AWS EC2 Systems Manager
Fleet management for vulnerability scanning and patching.

AWS Key Management Service (KMS)
Managed service to create and control encryption keys

Amazon Macie
Uses machine learning to automatically discover, classify, and protect sensitive data in AWS.

AWS Service Catalog & CloudFormation
AWS tools to manage approved services and environments across all accounts, Lines of Business, and user bases.

Amazon Inspector
Automated application security assessment service

AWS Cloud Hardware Security Module (HSM)
Hardware-based keys storage for regulatory compliance

AWS Identity & Access Mgmt. (IAM)
Securely control access to AWS services and resources for your users

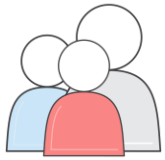
AWS Config & Config Rules
AWS resource inventory, configuration history, and configuration change notifications & preventive rules.

AWS Shield
Managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS

AWS WAF
Tool designed to filter malicious web traffic

amazon web services

AWS Compliance Program Compliance is a joint-effort



Customer

Responsibility for security *in* the cloud

- **Customer data**
- **Platform, applications, identity & access management**
- **Operating system, network & firewall configuration**
- **Client-side data encryption & data Integrity authentication**
- **Server-side encryption (file system and / or data)**
- **Networking traffic protection (encryption / integrity / identity)**

amazon web services

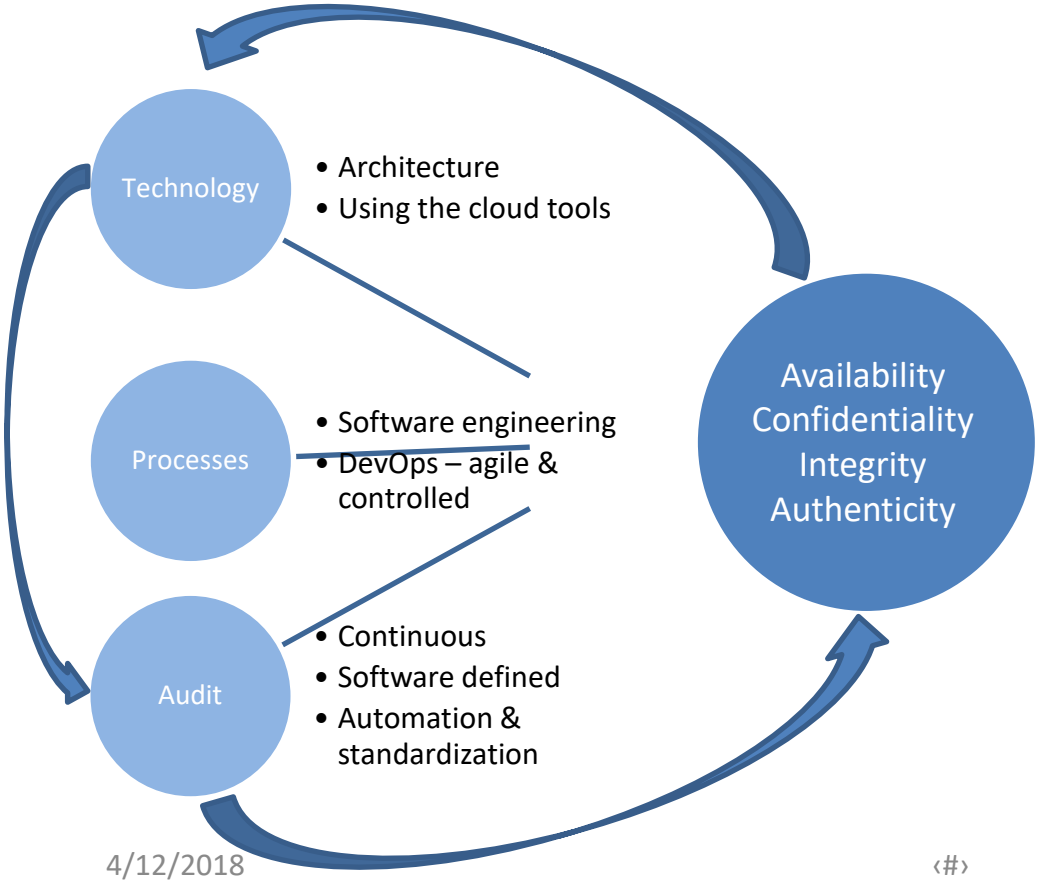
AWS

Responsibility for security *of* the cloud

- **Compute**
- **Storage**
- **Database**
- **Networking**
- **AWS global Infrastructure**
- **Regions**
- **Availability Zones**
- **Edge Locations**

amazon web services

AWS Compliance Program Risk Landscape



The customer is responsible for the correct usage of the „cloud“

The customer defines ACIA requirement

ACIA is the decision base for the architecture and is continuously auditable

Modernizing Technology Governance

1. Decide what to do (Strategy)

1.1 Identify Stakeholders

1.2 Identify Your Workloads Moving to AWS

2. Analyze and Document (outside of AWS)

2.1 Rationalize Security Requirements

2.2 Define Data Protections and Controls

2.3 Document Security Architecture

3. Automate, Deploy & Monitor

3.1 Build/deploy Security Architecture

3.2 Automate Security Operations

3.3 Continuous Monitor

3.4 Testing and Game Days

4. Certify

4.1 Audit and Certification

amazon web services

Security in the AWS Cloud

Amazon Virtual Private Cloud (VPC)

Amazon VPC lets you provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define.

AWS Direct Connect

AWS Direct Connect lets you establish a dedicated network connection between your network and one of the AWS Direct Connect locations. Using industry standard 802.1q VLANs, this dedicated connection can be partitioned into multiple virtual interfaces.

AWS Identity & Access Mgmt. (IAM)

AWS IAM enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

AWS Cloud Hardware Security Module (HSM)

The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) appliances within the AWS cloud. With CloudHSM, you control the encryption keys and cryptographic operations performed by the HSM.

S3 Server Side Encryption (SSE – S3)

With SSE-S3, Amazon S3 will encrypt your data at rest and manage the encryption keys for you.

SSE with Customer Provided Keys (SSE – C)

With SSE-C, Amazon S3 will encrypt your data at rest using the custom encryption keys that you provide.

SSE with AWS KMS (SSE– KMS)

With SSE-KMS, Amazon S3 will encrypt your data at rest using keys that you manage in the AWS Key Management Service (KMS).

AWS Key Management Service (KMS)

AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data, and uses Hardware Security Modules (HSMs) to protect the security of your keys.

AWS Config

AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. Config Rules enables you to create rules that automatically check the configuration of AWS resources recorded by AWS Config.

amazon web services

How AWS supports GDPR compliance (examples)

GDPR Art. 17: Data Portability

Network Connections, APIs, Snowball

GDPR Art. 32: Encryption

Encryption

Key Management Service

CloudHSM

Server-side Encryption

GDPR Art. 25: Data Access Control

Identity

IAM

Active Directory Integration

SAML Federation

GDPR Art. 17/30: Monitoring of processing

Compliance

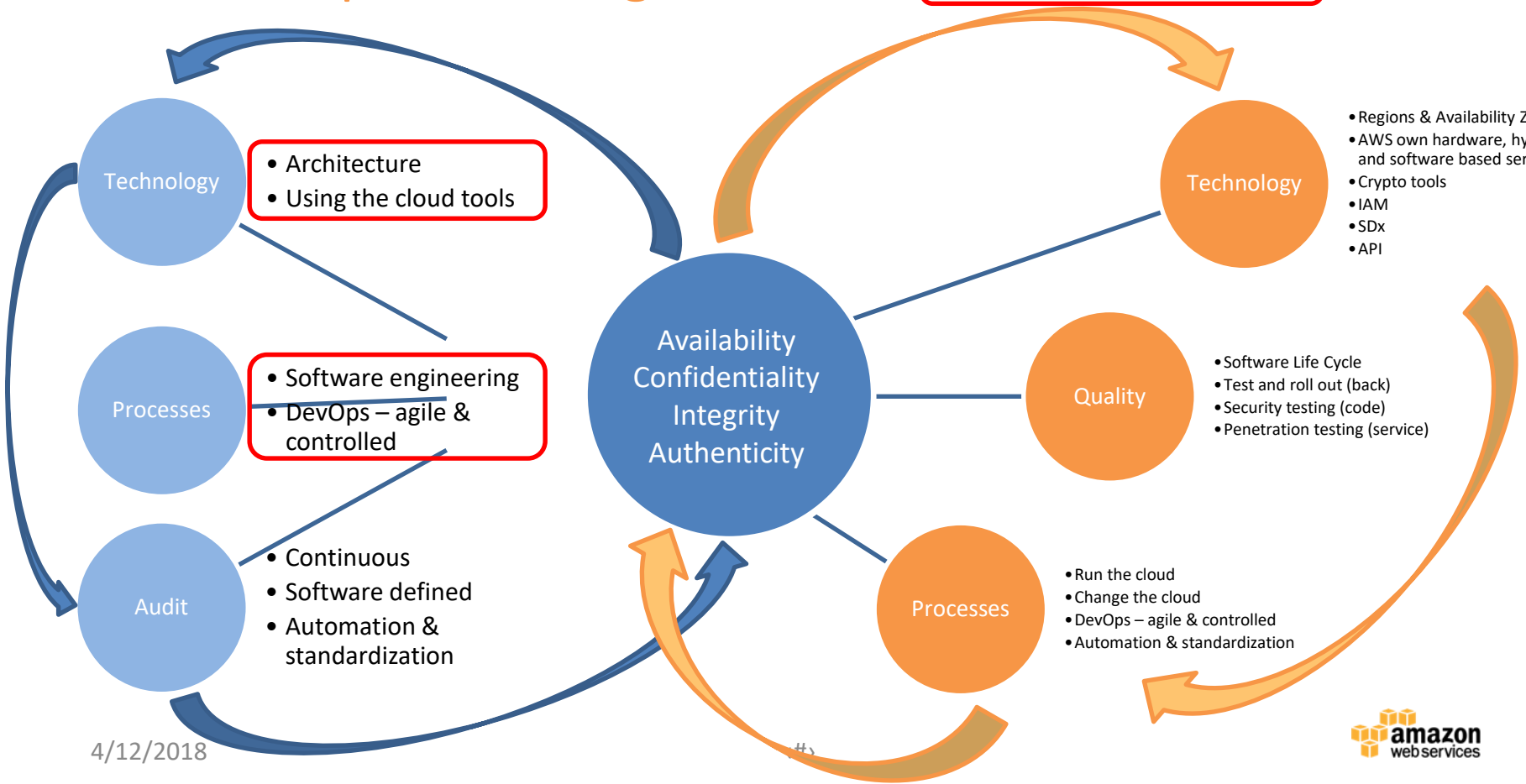
Service Catalog

CloudTrail

Config

amazon web services

AWS Compliance Program Risk – where to audit

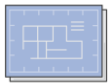


AWS Compliance Program Reduce infrastructure risk

Technical Account Manager enables enterprise-grade response times

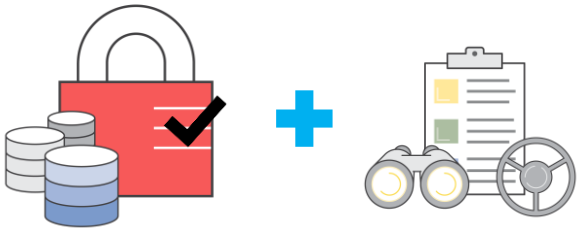
Operations Support provides root-cause analysis and reporting

AWS Trusted Advisor provides security and fault tolerance recommendations



Architecture Review increases reliability of existing and new applications

Infrastructure Event Management supports migrations and planned events



Robust security + **Effective governance**

amazon web services

WIE ERHÄLT MAN SEINE BETRIEBSSTABILITÄT UND COMPLIANCE

amazon web services

Data protection is a shared responsibility

Data Controller

Customers

Customer content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption

Server-side Data Encryption

Network Traffic Protection

DPA, Consent etc.

Data Subject

DPA, EU SCC

Data (Sub) processor

aws

AWS Foundation Services

Compute | Storage | Database | Networking

AWS Global Infrastructure

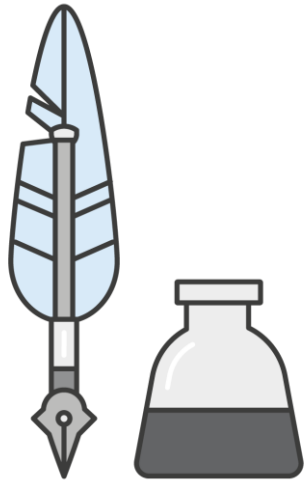
Availability Zones

Regions

Edge Locations

Data Processing Agreement/Addendum

- AWS has a GDPR-ready DPA available for customers today that is effective 25 May 2018.
- If applicable, any existing EU General Data Protection Directive DPA becomes invalid at midnight, 24 May 2018.
- Work with your AWS account team to obtain the AWS GDPR Data Processing Addendum.



aws
amazon web services

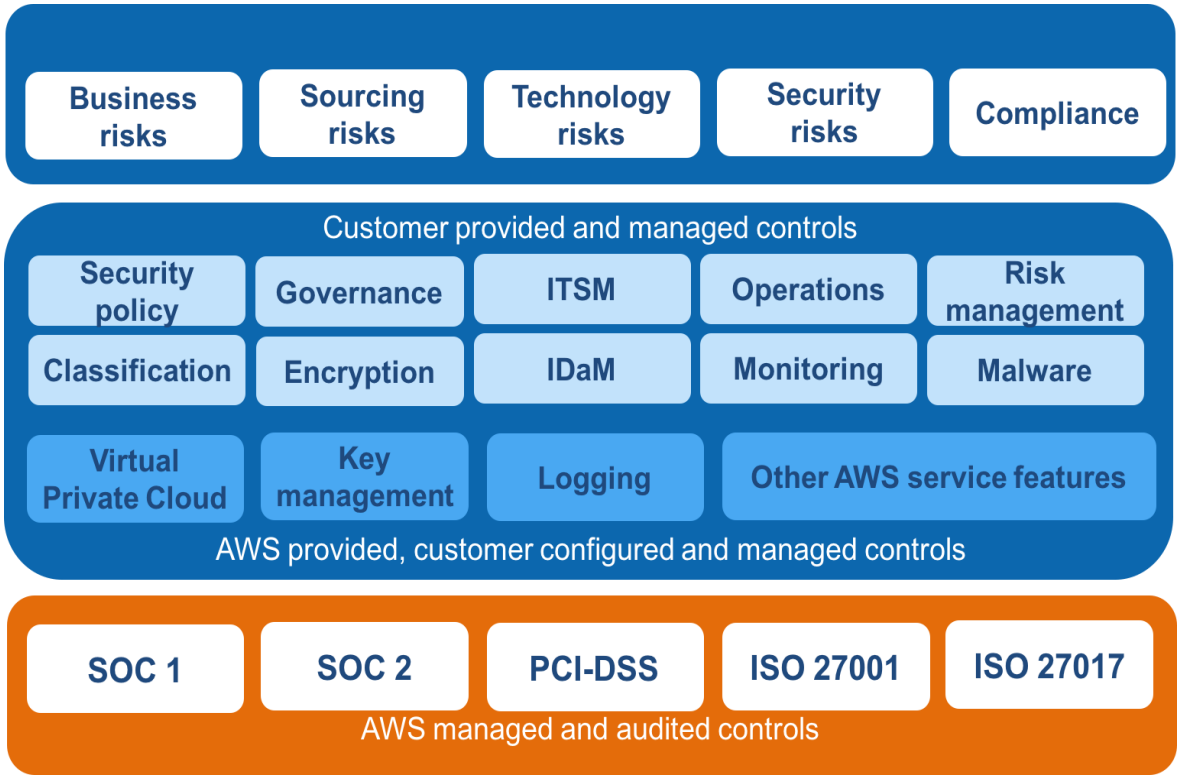
Governance in the Cloud

Customer risk management and desired control environment

Customers define the overall risk environment based on their internal and external requirements.

Customers decide on the appropriate controls and processes to manage and monitor the effectiveness of their customized AWS controls.

Based on the Customers' controls, companies can identify and document controls operated by AWS.



amazon web services

Modernizing Technology Governance

1. Decide what to do (Strategy)

1.1 Identify Stakeholders

1.2 Identify Your Workloads Moving to AWS

2. Analyze and Document (outside of AWS)

2.1 Rationalize Security Requirements

2.2 Define Data Protections and Controls

2.3 Document Security Architecture

3. Automate, Deploy & Monitor

3.1 Build/deploy Security Architecture

3.2 Automate Security Operations

3.3 Continuous Monitor

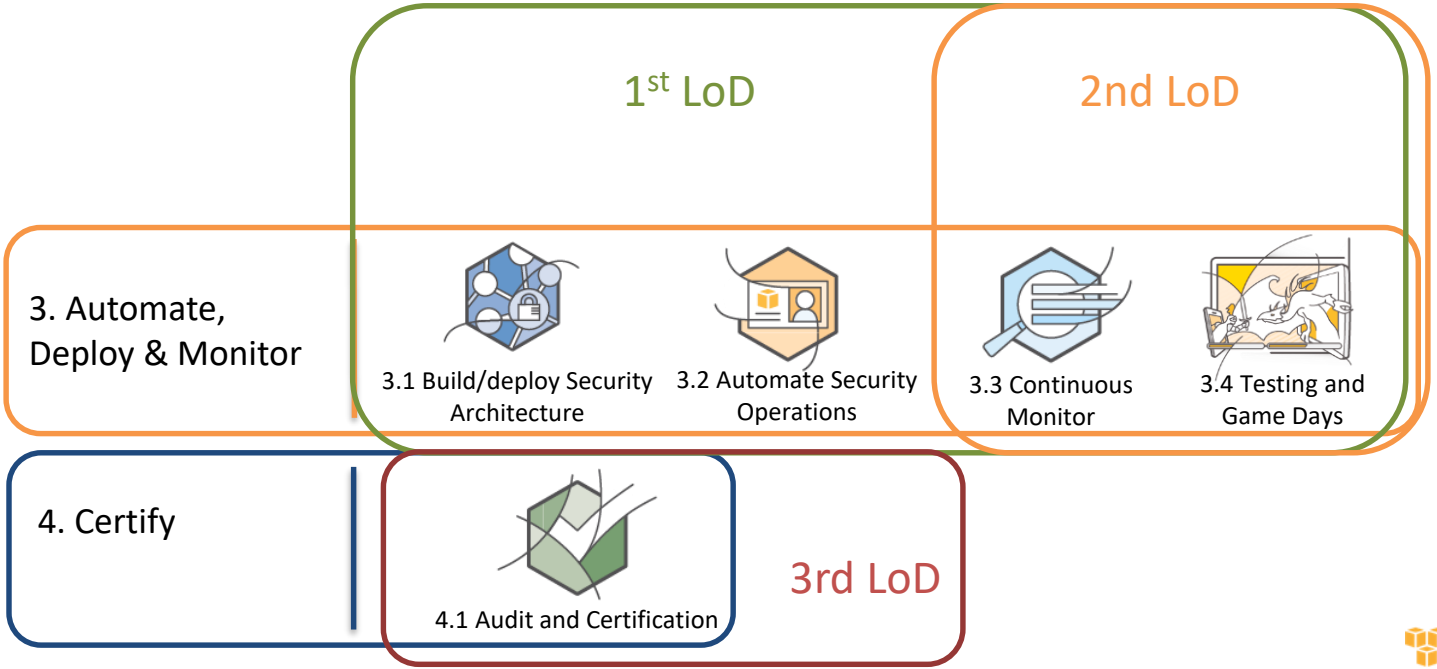
3.4 Testing and Game Days

4. Certify

4.1 Audit and Certification

amazon web services

Changes 3 Lines of Defense: Automation



Cloud Usage Examination

AUDITING ON AWS

amazon web services

AWS Auditing 5 Types of Audit Models

1. **Internal Testing:** Usually run by the Lines of Business, but needs to be automated
2. **Internal Audit:** You need to validate all the decisions made by your IT colleagues. Good and Bad.
3. **External Audit:** They need to be educated and trained before they show up and start poking around.
4. **Third Party Audit:** Use of AWS by SaaS providers is part of the program your regulators expect you to document.
5. **Regulatory Audit:** They will judge you on those things that you tell them you are doing. I.E. “we changed all our polices” or “we encrypt everything”.

Audit & Certification Programs – Core Components

CSA
Cloud Security Alliance Controls
Annually

ISO 9001
Global Quality Standard
Annually

ISO 27001
Security Management Standard
Annually

ISO 27017
Cloud Specific Controls
Annually

ISO 27018
Personal Data Protection
Annually

PCI DSS Level 1
Payment Card Standards
Annually

SOC 1
Audit Controls Report
Twice a Year

SOC 2
Compliance Controls Report
Twice a Year

SOC 3
General Controls Report
Annually

Criteria for AWS Availability Zone

ISO/IEC 27001:2013 Control objective A.17.2: Redundancies

ISO/IEC 27001:2013 Requirement A.17.2.1: Availability of information processing facilities

#	Controls Specified by AWS	Testing Performed by Independent Accountants
1.1	AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements.	Inquired of the Data Center Capacity Planning Senior Manager and ascertained that AWS maintained a capacity planning model that assessed current demand as well as forecasted future demand and availability. Selected a sample of months and obtained the capacity planning model review, ascertained that it was reviewed at least monthly, and contained forecasting for future demands and resource availability.
1.2	Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.	Inquired of Software Development Managers and ascertained that the production environment was monitored and that alarming was configured by Service Owners to notify operational and management personnel when early warning thresholds were crossed on key operational metrics. Selected a sample of key operational metrics and ascertained that related monitoring and alarming configurations existed and were configured to notify appropriate personnel when a threshold was reached or exceeded.
1.3	AWS systems are designed with redundancy to tolerate isolated faults and loss of a datacenter without interruption to the service.	Inquired of the AWS Compliance Program Manager and ascertained that AWS systems were designed with redundancy to prevent the interruption of service due to loss of a data center within a region. Selected a sample of data centers and ascertained that they were geographically separated from other data centers within the same region. Inspected the architecture of the service activity logging tool and ascertained that the service was designed to store data using redundant object storage.

Examples of access control and testing

1.7	EC2-Specific – AWS prevents customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software.	Inquired of an EC2 Security Manager and ascertained that customers were restricted from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. Observed an EC2 Security Engineer attempt to ping the physical host from an instance within the host and ascertained that the physical host was isolated from instances. Observed an EC2 Security Engineer attempt to access a file stored on an instance while logged into the physical host the instance was located on and ascertained that the physical host was unable to access specific instances.

#	Controls Specified by AWS	Testing Performed by Independent Accountants
1.8	EC2-Specific – AWS prevents customers from accessing EBS volumes and private snapshots of EBS volumes that are not assigned to them via access permissions.	Inquired of an EC2 Security Manager and ascertained that customers were restricted from accessing EBS volumes and private snapshots of EBS volumes not assigned to them through access permissions. Logged into an AWS account and ascertained that an EBS volume and private snapshot belonging to another AWS account could not be accessed unless the necessary permissions were granted to the account. Using the account to which the snapshot belonged, we granted permissions to the alternate account and subsequently confirmed the snapshot could be successfully accessed.

1.3	System activities are logged, retained for a defined period of time and protected from unauthorized modifications.	Inquired of the AWS Compliance Program Manager and ascertained production system activities were logged, retained, and configured with logical access controls to restrict access to logs and protect audit information from unauthorized modification and deletion. Inspected the administrative configurations for the log aggregation tools and ascertained that service activity was logged and service team users were unable to delete or modify log records.

Artifact - the self service portal for official compliance documents


amazon
web services
Financial
Services

Thank You


amazon
web services

AWS Auditing Key Enabling Resources

- Auditor Learning Path
  - https://aws.amazon.com/compliance/auditor-learning-path/
- Introduction to Auditing the Use of AWS
  - https://d0.awsstatic.com/whitepapers/compliance/AWS_Auditing_Security_Checklist.pdf
- Operation Checklists for AWS
  - http://media.amazonwebservices.com/AWS_Operational_Checklists.pdf
- AWS Security Audit Guidelines
  - http://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html
- AWS Security Best Practices
  - https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

AWS Compliance Program Key Technical Resources

- Website: AWS Cloud Compliance Home Page
- Website: PCI DSS 3.2 Resource Home Page
- Website: AWS CIS Benchmarks for Core Systems & Applications
- Whitepaper: AWS Risk & Compliance
- Whitepaper: AWS Certifications, Programs, Reports,
- Whitepaper: AWS Answers to Key Compliance Questions
- Whitepaper: AWS CSA CAIQ Guide
- Examination Guide: AWS FFIEC IT Handbook Guide

amazon web services

Security Assurance Tool Descriptions

AWS provides financial services customer a significant number of **“on-platform”** tools to manage their security & compliance operations. Some of the key elements are:

- AWS Trusted Advisor provides real time guidance to help you provision your resources following AWS best practices.
- AWS Cloud Trail tracks API call history and the results enable security analysis, resource change tracking, and compliance auditing.
- AWS CloudWatch allows you to track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.
- AWS Config & Config Rules are fully managed services that provide you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance.
- AWS Service Catalog allows you to control which IT services and versions are available, the configuration of the available services, and permission access by individual, group, department, or cost center.
- Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices.

amazon web services

Simmons & Simmons

simmons-simmons.com
elexica.com