Cloud Security & Compliance
A focus on Governance

Tim Rains
Regional Leader, Security & Compliance Business Acceleration
Worldwide Public Sector, Amazon Web Services
Agenda

Traditional Information Security Governance

Security & Compliance Game Changers

Governance Improved
Initially contemplating the cloud

- On-premises control equivalency: support for current controls/vendors?
- Data protection: what controls prevent unauthorized access?
- Multi-tenancy: is there any new risk from other tenants?
- Data residency: will our data move outside of a specific country/region?
- Resilience: can it meet our requirements?
- Governance: support for the framework(s), policies and controls that help us manage risk?
Traditional Information Security Governance
Traditional Governance Flow

Strategy
Traditional Governance Flow

Strategy

Policy
Traditional Governance Flow

- Strategy
- Policy
- Project Team
Traditional Governance Flow

- Strategy
  - Policy
  - Project Team
  - Governance
Traditional Governance Flow

1. Strategy
   - Policy
   - Project Team
   - Governance
   - Check
Traditional Governance Flow

1. Strategy
2. Policy
3. Project Team
4. Governance
5. Audit
6. Check
Traditional Governance Flow

1. **Strategy**
   - Policy
2. **Project Team**
3. **Governance**
   - Audit
4. **Check**
5. **Release!**
Traditional Governance Flow

Strategy ➔ Policy ➔ Project Team ➔ Governance ➔ Check ➔ Release!

Governance ➔ Audit ➔ Archive

Policy ➔ Governance ➔ Check ➔ Release!
Traditional Governance Flow

- Strategy
- Policy
- Governance
- Audit
- Check
- Release!

Project Team
Security & Compliance
Game Changers
- Independent geographic areas, isolated from other Regions (security boundary)
- Customer chooses in which Region(s) to deploy services
- Regions are comprised of multiple Availability Zones (AZs), which enables the deployment of high-availability architecture
- AZs are independent failure zones; physically separated; on separate low risk flood plains
- Discrete Uninterruptible Power Supply (UPS); Onsite backup generation facilities
- Built for continuous availability
AWS Global Infrastructure

The AWS Cloud spans 66 Availability Zones within 21 geographic Regions around the world, with announced plans for 12 more Availability Zones and four more Regions in Bahrain, Cape Town, Jakarta, and Milan.

Europe / Middle East / Africa

- **Europe (Ireland) Region**
  - EC2 Availability Zones: 3
  - Launched 2007

- **Europe (London) Region**
  - EC2 Availability Zones: 3
  - Launched 2016

- **Europe (Stockholm) Region**
  - EC2 Availability Zones: 3
  - Launched 2018

- **Europe (Frankfurt) Region**
  - EC2 Availability Zones: 3
  - Launched 2014

- **Europe (Paris) Region**
  - EC2 Availability Zones: 3
  - Launched 2017
Amazon CloudFront uses a global network of 180 Points of Presence (169 Edge Locations and 11 Regional Edge Caches) in 69 cities across 30 countries.

Europe

Edge locations: Amsterdam, The Netherlands (2); Berlin, Germany (2); Copenhagen, Denmark; Dublin, Ireland; Frankfurt, Germany (8); Helsinki, Finland; London, England (9); Madrid, Spain (2); Manchester, England; Marseille, France; Milan, Italy; Munich, Germany (2); Oslo, Norway; Palermo, Italy; Paris, France (5); Prague, Czech Republic; Stockholm, Sweden (3); Vienna, Austria; Warsaw, Poland; Zurich, Switzerland

Regional Edge caches: Frankfurt, Germany; London, England
Things are different in the cloud

**On-premises**
- Big perimeter
- End-to-End ownership
- Build it all yourself
- Server-centric approach
- De-centralised administration
- Focus on physical assets
- Multiple (manual) processes

**On AWS**
- Micro-perimeters
- Own just enough
- Focus on your core values
- Service-centric approach
- Focus on protecting data
- Central control plane (API)
- Everything is automated
Game changer: everything is automated

- Infrastructure as Code
- Configuration as Code
- Policy as Code
The changing nature of security

Secure development lifecycle applies equally to applications and *infrastructure as code*
Game changer: API-driven

• Authoritative - the interface to, and between, AWS services
• Auditable – always know what, and who, is doing what
• Secure – verified integrity, authenticated, no covert channels
• Fast - can be read and manipulated in sub-second time
• Precise – defines the state of all infrastructure and services
• Evolving – continuously improving
• Uniform - provides consistency across disparate components
• Automatable - enables some really cool capabilities
You are making API calls on a growing set of AWS services around the world. CloudTrail is continuously recording API calls. The recorded data can be stored/archived and used for troubleshooting and monitoring & alarm purposes.
AWS Config and AWS Config Rules

A continuous recording and assessment service

Answer the questions:
How are my resources configured over time?
Is a change that just occurred to a resource, compliant?
Automating Responses Based on Multiple Controls

- AWS CloudTrail
- VPC Flow Logs
- Amazon GuardDuty
- Amazon Macie
- AWS Config
- Amazon CloudWatch Events
- Lambda function
- AWS APIs
- Team collaboration (Slack etc.)
- Amazon Inspector

Detect
Investigate
Respond
Governance Improved
Governance At The Speed Of Cloud

- Strategy
- Policy
Governance At The Speed Of Cloud

Strategy

Policy

Project Team
Governance At The Speed Of Cloud

Strategy → Policy → Project Team → Automated Checks
Governance At The Speed Of Cloud

- Strategy → Policy → Project Team
- Automated Checks
Governance At The Speed Of Cloud

- Strategy
- Policy

- Project Team
- Automated Checks
- Release!
Governance At The Speed Of Cloud

Strategy

Policy

Project Team

Automated Checks

Compliance Data

Release!
Governance At The Speed Of Cloud

- Strategy
  - Policy
    - Project Team
  - Compliance Data
    - Automated Checks
      - Release!
Governance At The Speed Of Cloud

Strategy

Governance

Policy

Compliance Data

Automated Checks

Project Team

Release!
Governance At The Speed Of Cloud

- Strategy
- Policy
- Project Team

Governance

Automated Checks

Compliance Data

Release!
Governance At The Speed Of Cloud

- Strategy
- Policy
- Project Team

Governance

Compliance Data

Automated Checks

Ops

Release!
Governance At The Speed Of Cloud

- Strategy
- Policy
- Project Team
- Automated Checks
- Compliance Data
- Governance
- Audit
- Ops
- Release!
Governance At The Speed Of Cloud

- Strategy
- Policy
- Project Team
- Governance
- Automated Checks
- Compliance Data
- Audit
- Ops
- Release!
Certifications, Attestations, Standards
All AWS Services GDPR ready
by Chad Woolf | on 26 MAR 2018 | in Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS Config, Compliance, Security, Identity, & Compliance, Webinars | Permalink | Comments | Share

Today, I’m very pleased to announce that AWS services comply with the General Data Protection Regulation (GDPR). This means that, in addition to benefiting from all of the measures that AWS already takes to maintain services security, customers can deploy AWS services as a key part of their GDPR compliance plans.

This announcement confirms we have completed the entirety of our GDPR service readiness audit, validating that all generally available services and features adhere to the high privacy bar and data protection standards required of data processors by the GDPR. We completed this work two months ahead of the May 25, 2018 enforcement deadline in order to give customers and APN partners an environment in which they can confidently build their own GDPR-compliant products, services, and solutions.

https://aws.amazon.com/compliance/gdpr-center
Survey: Please Give Us Feedback!

https://amazonmr.au1.qualtrics.com/jfe/form/SV_9RILSIJHhzBi5zn
Thank you!

Tim Rains
rainstim@amazon.co.uk