Compliance != Security
Compliance != Security
but we used it anyway

Robert Clark, IBM Cloud
Compliance != Security
but we used it anyway and
improved the way we deliver
devops security for agile
teams at scale

Robert Clark, IBM Cloud
My service is ready for production, where do I get my compliance certifications?
My service is ready for production, where do I get my compliance certifications?

That depends, is it secure?
My service is ready for production, where do I get my compliance certifications?

That depends, is it secure?

Probably!? Isn’t that what certifications are for?
Conversations

Every Security Person
Transformation
Challenges

Acquisition Maturity
DevOps Security
Compliance Limitations

How we Staff

How we Build
Our Cloud Agility Model

Similarities with the “Spotify Model”

DevOps - Design, Build, Ship, Maintain

Self sufficient squads

Squads grouped into tribes
Acquisition Maturity

Solo Security Engineer

Fully Staffed Security Team
Anatomy of a Squad

Tribe Leader

Developer  Systems Engineer  Automation Engineer  Offering Manager  Security Engineer  Experience Assurance
How do we enable small squads to deliver security?
Compliance != Security
How do we make IT less scary?
Compliance

Prove we know what we’re doing?

How do we make IT less scary?

Demonstrate safety and best practice?
Prove we know what we’re doing?

Demonstrate safety and best practice?
Will COMPLIANCE save us?
Let's get our squads doing compliance!
Compliance
Indifference
Anger
Denial

By Rexness from Melbourne, Australia (Meerkat digging) [CC BY-SA 2.0 (https://creativecommons.org/licenses/by-sa/2.0)], via Wikimedia Commons
Exodus
Challenges

How do we make compliance accessible?
INDUSTRY POP QUIZ

EQUIFAX

Bell

SABRE

UBER

Yahoo!

Verifone

TARGET

IHG

Atlassian

HipChat

Whole Foods Market

Deloitte

Oracle

micros

Wonga

3

Virgin America

Nissan

Transportation Security Administration
List of data breaches and cyber attacks in October 2017 – 55 million records leaked

A story I want to surgery firm. A w list of patients, a worrying for the the royal family, criminals have.

So, numbers: by October. But, as
Compliance Misconceptions
Compliance Misconceptions
COMPLIANCE

Controls Based Planning
Evidence Driven Documentation
Defining Processes

GOOD FOR

Enforcement of Security
Technical Innovations

BAD FOR
Challenges

Understand the limitations of compliance
How do we build for security in a cloud native world...

... if “compliance” isn’t the answer?
Changes

How we Staff
Centralized Expertise
Oriented to Controls
Distributed Security Function

800-53
Common Control Alignment

How we Build
Measurable Controls
Optional Services
Integrated Tools
NIST Alignment

800-53 Security & Privacy Controls and Cyber Security Framework

- Superset of Common Controls
- Strong Privacy Controls (R5)
- Federal Bedrock
- Significant Internal Alignment
- Customizable
- Variable Maturity Model

Identify - Protect - Detect - Respond - Recover
BUILD A CENTRAL TEAM OF TALENT

Service Security Squads

Security Talent
<table>
<thead>
<tr>
<th>FAMILY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
</tr>
<tr>
<td>Awareness &amp; Training</td>
</tr>
<tr>
<td>Audit and Accountability</td>
</tr>
<tr>
<td>Assessment, Authorization and Monitoring</td>
</tr>
<tr>
<td>Configuration Management</td>
</tr>
<tr>
<td>Contingency Planning</td>
</tr>
<tr>
<td>Identification and Authentication</td>
</tr>
<tr>
<td>Individual Participation</td>
</tr>
<tr>
<td>Incident Response</td>
</tr>
<tr>
<td>... [11 more control families]</td>
</tr>
</tbody>
</table>
Aligning Talent

- FAMILY
- Access Control
- Awareness & Training
- Audit and Accountability
- Assessment, Authorization and Monitoring
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Individual Participation
- Incident Response
- ... [11 more control families]
Control Expertise
Things we have strong opinions about and **know how to measure**

Functional Delivery
Things we do and **deliver** to benefit cloud services and engineers
Security Focal Program

**Role:** Security Focal

**Participation:** Part Time

**Responsibilities:**
- Attend NIST Aligned Security Training
- Participate in Security Reviews
- Support IR and Vulnerability Management
- Know enough to ask for help

**Role:** Tribe Security Leader

**Participation:** Full Time

**Responsibilities:**
- Security of portfolio segment
- Support their Security Focals
- Escalation point for service / tribe issues
- Owner of local security budget
This person *owns* security for their tribe.

These people deliver security for their services.
Lessons Learned

Not every squad has an aspiring security ninja

NIST is a really big standard!

Focus must always be on developers

Secure the path of least resistance
Our Results

- Accelerated Penetration Testing
- Incident Response
- Centralized Talent
- Security Career Path
- Enhanced Service Delivery
- Better Communications
- Enhanced Tooling
- Scaled Threat Modelling
- Clearer Positioning
- Enabled Developers
Happy Developers
What's Next

Which other standards would work?

Where are the DevOps Security tools?

How much can we really measure?
Questions
Our Results

- Enhanced Service Delivery
- Best-in-Breed Tooling
- Better Communications

- Accelerated Penetration Testing
- Incident Response
- Consolidation

- Centralized Talent
- Security Career Path
- Scaled Threat Modelling
- Clearer Positioning

- Enabled Developers
How we build

AGILE

SECURITY

DevOps