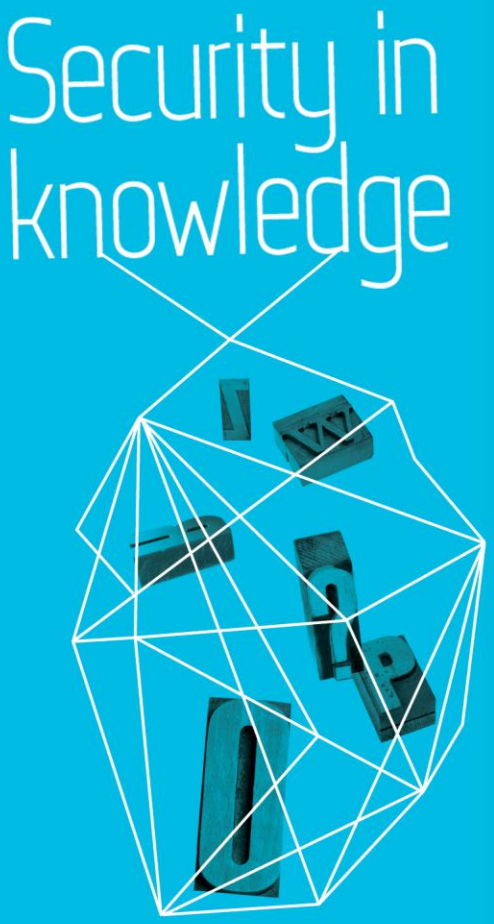


Implicit Risk Management – When is "Good Enough" Sufficient?

Bill Burns
Netflix

Ben Tomhave
LockPath

Session ID: GRC-W25B

Session Classification: Intermediate

To Wit. . .

"To measure is to know."

"If you can not measure it, you can not improve it."

– Sir William Thomson (Lord Kelvin)

Netflix Snapshot

- 33 million global members
- Streaming in 40 countries
- ~1B hours streamed/month
- Available on ~1000 devices
- Netflix streaming is 1/3rd of US evening Internet traffic

High Performance Culture

- Engineering-Centric
  - DevOps / NoOps – you own it!
  - Fail Fast, Learn Fast… Get Results
  - Empowered Employees = Faster Innovation
- Core Values:
  - "Freedom & Responsibility"
  - "Highly-Aligned, Loosely-Coupled"
  - "Over-Communicate"
  - "Context, Not Control"
  - Courage & Judgment

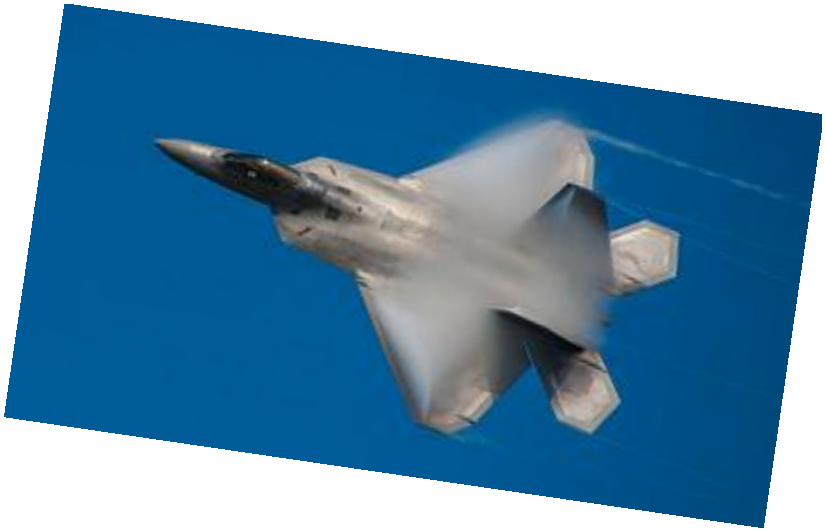
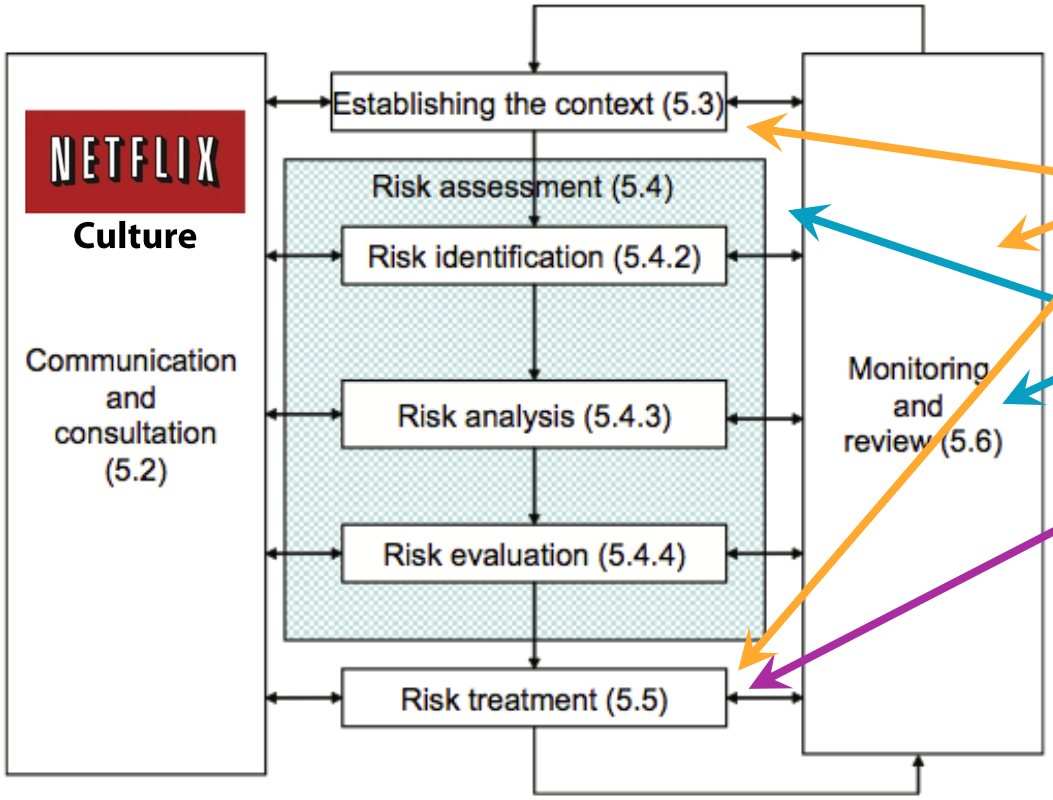


Photo: http://www.flickr.com/photos/72213316@N00/7674481990/sizes/n/in/photostream/

NETFLIX

Lockpath

"Good Enough" RM Examples



3. Baked-In Tools

1. Aggressive Testing

2. Integrated Vuln. Mgmt.

ISO/IEC 31000:2009 Risk Management Process

Addressing Availability Risk

- Assume Failures
  - If you fear a failure mode, find a way to automate testing for it
- Aggressively Test
  - Chaos Monkey/Gorilla
  - Intentionally inducing failures
  - Helps practice recovery
- No free pass for security!

Photo: Bettmann/Corbis

NETFLIX

Lockpath

Addressing Vulnerabilities

- Goal: Running instances do not get patched
- Alternative:
  - Bake a new AMI
  - Launch, test new instances in parallel
  - Kill old instances
- End Result: Winning!

Photo: http://si.wsj.net/public/resources/images/OB-UA904_0805bo_G_20120805170407.jpg

Addressing Tool Adoption

- Controls baked into templates
  - Place controls near the data
  - Automation ensures coverage
- Cloud/DC agnostic security controls
  - Provides a single view of attack surface
  - Evolving, work in progress
- Secure option = Easy option

Photo: http://www.flickr.com/photos/karen_roe/8191728662/sizes/m/in/photostream/

Concluding Thoughts

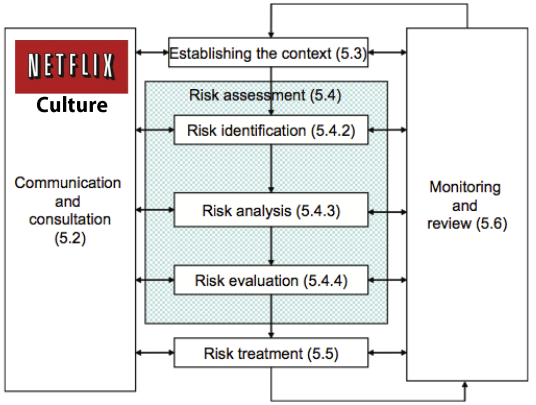


Figure 3 — Risk management process

- Cloud+DevOps → Different RM Context
- Continuous testing → Resilient code
- Security controls are baked-in
- Replacement instances look just like the originals
- Everyone is accountable for excellence

Automation = Conformity & Consistency

Thank you!

Bill Burns
biburns@netflix.com

Ben Tomhave
ben.tomhave@lockpath.com