FLOWCON
CONTINUOUS DESIGN DELIVERY DATA

Audits of High Deployment Environments

A discussion

@jdeluccia

FOLLOW US @FLOWCONSF

Speaker

- James DeLuccia
  - EY Americas lead certification services
    - Translated: “executive on every ISO engagement”
  - Clients mainly technology – software & device
  - Author
  - Tinkerer .. Recovering coder; product manager; startup junkie

AUDIT SPEAK

Format

- *Present* Industry, Business, Management, or Auditor requirement
- *Speak* from hypothetical non-existent client demonstrative examples
- *Highlight* analogies or translations of initial requirement

Role of Assurance

- Businesses must find a level of trust between each other … 3rd party reports provide that confidence. Those issuing the reports stake their name & liability with each issuance
- Translated:
  - OAuth for business

Types of audits

- Internal / External / Vendor / Statutory
- Scope and bounds
- Recipient of report: Stock market, your management, regulators, investors, business partners, vendors, and clients
  - >> Each has a unique concern and right

Audit report trends

- Requirement & scrutiny increasing
- MORE vendors and clients mandating
- Regulations and quality standards are catching up to ~~roughly~~ ~~2001~~ technology
- Study shows:
  - ¾ of organizations seeing increased requests
  - ~45% of existing audit reports do not satisfy client requets → requiring manual re-work

Why are auditors asking for these things?

- Birth of audit requirements:
- Birds and the bees:
  - Regulations & other stated 3rd parties transfer risk to your business and ask for proof that such is addressed sufficiently to place reliance on your business operations
  - Which results in CONTROL OBJECTIVES

"*12.1.4 Separation of development, testing and operational environments*"

- Control Objectives are further elaborated:
  - *"Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment."*
- But what does this MEAN for me?
  - That is for you to decide …

What does it take?

- How you execute to meet the Control Objective is unique
- Procedures are generally in place and documented supporting this control
- THAT is what the auditor needs .. And your help is paramount.

What auditors need

- Demonstrative evidence that a ‘Control Objective’ is satisfied to a statistically relevant level
- Translation:
  - Clean ability to understand how Management risks are addressed within the deployed technology

Coming down the track; Left the station, and running you down

LETS TALK ABOUT TRAINS

Key Activities: Coming down the tracks

- Control Objectives, Procedures, and ultimately the audit activities originate from:
  - Risk assessments: Threat & Vulnerabilities tied to controls to mitigate them
  - Design of security program itself
- Participating in what these risks are .. How the business addresses those is a two way track (both the program & audit benefit from two way communication and change)

Key Activities – once the train has left the station

- As a team, seek out the regulatory and common control objectives the business is managing against
- Identify any procedures already committed and develop translation of those procedures to your environment – and GET sign off
- Compose evidence repository of past 12 months and set strict read/write permissions for evidence usage

Key Activities: During audit

- Not possible to change the audit control objectives and underlying procedure
- Not representing controls is a negative event and expensive
- Remember – the control & evidence being tested is based upon the business' view of risk .. Not the auditors, you both have same objective

Discussion and examples

CHALLENGING ENVIRONMENTS

Fact or fiction

- Utilize the audit as part of continuous improvement
  - Require a feedback function to help program year over year
- Providing evidence that “shows” what was asked, but doesn’t address the control risk only ultimately hurts the business & you

Change Management

- Preventive vs. Detective Controls
- Tier out your Changes
  - Based on what?
  - Responsive control structures
- Visibility
- How to transform organization from 2 week change to > 2 hour

Separation of Duties

- It is possible to have both worlds
- 2 paths
  - Deep separation (example: Netflix)
    - Multi-levels of accounts, monitoring, and prescriptive controls
  - Wicked good automated applications acting as “promoter”, so there is a central coordinated method of monitoring, tracking, and auditing

PCAOB Updated 10/24/2013

- SOX and CD
  - Risks must be assessed to prevent material misstatement of significant account & disclosures
    - It was found in prior years management controls and monitoring controls tested did not satisfy this requirement
  - Identify areas of potential misstatement – types and likelihood

2012 Inspector observation

- "Testing a sample of locations and extrapolating the results of that testing to other locations without performing procedures to evaluate whether the issuers' systems and controls were **designed and implemented consistently across all of those locations**"

What is a clean auditable world?

- Clarity
- 100% awareness
- Multiple competencies involved
- Reproducible
- Comparable
- Integrity / Validity