Consolidating Compliance Audits in Order to Improve Efficiency and Improve Risk and Compliance Posture

Andrew Williams, Lead, Coalfire

Professional Strategies – S11

Agenda

- Introduction
- Quick Background
- Trends in Industry
- Challenges Presented by these Trends
- How Coalfire has Responded in the Past
- Our Lessons Learned
- What We've Settled On

Introduction

- Not a new issue: the concept of a company combining different compliance objectives and risk management into an integrated program has been around for some time
- Traditionally, this has been very difficult to do
- Today, I'll share how we've responded in the past, why we settled on our current process, and some of our lessons learned

Quick Background

- At Coalfire, our push for consolidation was initially born out of a quest for efficiency
- We were also having trouble effectively providing clients advice on how to leverage compliance to address system-wide risk, not just framework risk
- We began to see several other trends that make program integration a must-do for many companies

First Trend: Check Boxes

- In the past, many enterprise, cloud and on premise IT programs have thought of compliance as a check box
- Breaches across the IT landscape have changed the game
- ‘Complying with PCI’ is not the same as ‘securing customer data’.
- Challenge #1: Compliance ≠ Security

Second Trend: Risk Visibility

- Customers often contract us to help with a specific compliance objective, and then ask the question "What can I do to make myself secure?"
- Challenge #2: Working with a given compliance framework only provides a partial or specific context for system risks.

Third Trend: Cloud

- Compliance in the Cloud becomes an issue of differentiation
- Attempting to keep up with compliance coverage of competitors can result in missed expectations and immense overhead.
- Challenge #3: Compliance programs are hard to scale efficiently

Three Challenges

- Challenge #1: Compliance ≠ Security
- Challenge #2: Working with a given compliance framework only provides a partial or specific context to external risks.
- Challenge #3: Compliance programs are hard to scale efficiently

Different Responses

- In response to these trends, Coalfire went in several different directions (and our clients tend to do the same):
  - #1 Head in the sand
  - #2 Compliance Framework Mappings
  - #3 Enterprise GRC Tool Deployment

Response #2: Control Mapping

- Pros:
  - Excellent thought exercise to identify common compliance and security concerns
  - Effective tool for comparing coverage
- Cons
  - 'Legally Defensible' is hard to ensure
  - Hard to scale, quickly become unmanageable

Response #3: GRC Tools

- Pros
  - Provide extremely powerful audit and risk management tools
  - Feasible to use operationally
- Cons
  - Often extremely expensive
  - Rendered ineffective if deployed or managed incorrectly, which seems to happen often

What's the answer?

- In response to these trends, Coalfire went in several different directions (and our clients tend to do the same):
  - #1 Head in the sand
  - #2 Compliance Framework Mappings
  - #3 Enterprise GRC Tool Deployment
  - #4 Artifact and Cadence-based Approach

Our Current Approach

- At Coalfire, we have moved from a control-based workflow for integrated assessments to an artifact and cadence-based workflow for integrated programs
- Same deliverables and findings, but different methodology

Current Approach (cont.)

- At its core, the issue boils down to one of project management
- Impossible to project manage based on semantics and shaky legal ground (control mappings)
- Unfeasible to project manage by throwing money at the problem (GRC enterprise tools)

Current Approach (cont.)

- We started by identifying the least common denominators
  - Evidence
  - Program / framework level discovery limitations
  - Control cadence
- Iterated a few times, and
- We had a program! In hindsight, an easily replicable process.

Results

- We have been able to leverage this approach to respond much more effectively to the trends we see
- Helps us move past an issue that been an obstacle for us for a long time
- Refocuses us (and by extension our clients) on risk and security posture, instead of worries about compliance overhead and barriers to entry

Three Challenges

- Challenge #1: Compliance ≠ Security
- Challenge #2: Working with a given compliance framework only provides a partial or specific context to external risks.
- Challenge #3: Integrated programs are hard to scale efficiently

Questions?