Consolidated Audit Program (CAP)
A multi-compliance approach

ISSA CONFERENCE

Carlos Pelaez, Director, Coalfire

May 14, 2015

About Coalfire

We help our clients recognize and control cybersecurity risk, maintain compliance with all major industry and government standards, and provide automated threat assessment solutions. Providing clients with:

- Detailed risk assessment that outlines immediate threats and how to manage gaps in security operations
- More experience, with the average consultant holding 4-5 IT certifications and over 10 years of industry expertise
- Managed costs through Consolidated Audit Program across PCI/HIPAA/FISMA/SOC/ISO and more

Coalfire

Part One (11AM)

- Why are we talking about this?
- Compliance Challenges
- Consolidated Audit Program
- Reducing Cost and Risk

Part Two (3PM)

- UCF Defined
- UCF Demo
- Example work product
- Questions

Coalfire

Consolidated Audit Program (CAP) Explained

PART ONE

Coalfire

Why are we talking about this?

- Are we secure?
  - Board of Directors/Management asking questions
  - Technology outpacing compliance
- Who do you work with?
  - Dependence on 3rd parties
  - Service providers demand compliance evidence

Coalfire

Challenges for compliance teams

- IT security and compliance budgets
  - Need to do more with less
  - Focus on risk
  - Regulations and standards increasing in number and com
- Subject matter expertise hard to find
  - Need for control mapping comes in bursts
  - Takes time to update controls when standards refresh
  - What-if scenarios out of reach
- Existing GRC tools do not offer enough functionality
  - Need to focus on embedding controls in organization's DNA
  - Need to define clear ownership of controls
  - Need to associate assets and make an inventory for cyber security

Coalfire

Methodology Explained

CONSOLIDATED AUDIT PROGRAM

Coalfire

CAP from Customer Perspective

- **CAP is an abstract concept**
- **CAP is not governed by any regulation, standard, or governance body**
- **CAP is often what a customer wants, but cannot articulate**
- **CAP seems intuitive**

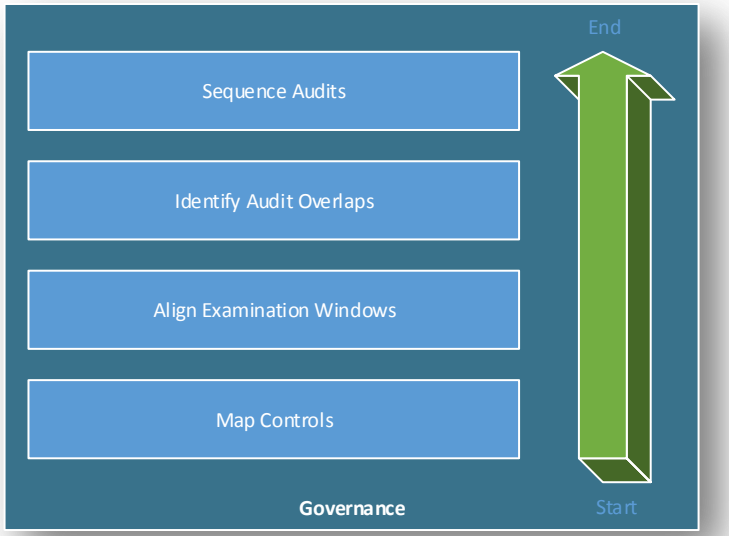
Example 1 – Surely there must be a better way to get all the audits done
Michelle has worked in compliance for over 10 years. She started her career at a global accounting firm and is most comfortable with Sarbanes-Oxley. As head of compliance for a Fortune 500 company, she now oversees all areas—including PCI, Healthcare, and SOC. Her financial acumen and audit experience tells her that there must be a way to trim some costs and make it easier for her to manage the teams of compliance staff across the US, which total 10 in her department. She reports to the VP of Internal Audit and he has asked her to be smart about the budget, but also to try to make sure she is thinking of new ideas to make the process easier.

Example 2 – Working through the compliance hoops is tough, so we are starting with PCI
Jack started his career managing the network and computer systems for a large university. With the boom of the internet, he was able to take a key job for Y2K in the MIS department of a Fortune 500 company. After a recent restructure, he was move into the compliance area with a focus on IT security. PCI is his key area of interest for the national retailer he works with and he is gathering bids. Later in the year, he wants to do Healthcare and ISO. He wants to know that he is secure. In his view, his team is not technical enough, but they do their best.

Coalfire

CAP Methodology

- Governance
- Mapping Controls
- Aligning the Examination Windows
- Identifying Audit Overlaps
- Sequencing Audits



Governance

What to do:

- Don’t go straight to the market
- Identify who signs off on each compliance report
- Consider the impact of failing a Common Control
- Centralize a Point of Contact
- Select one compliance domain to be the anchor
- Consider using Internal Audit as an internal orchestration mechanism
- What will the escalation process be?
- Map out the objectives and communicate these early on in the process

Coalfire

Understand What is in Scope

Fully understand the domains in scope

- Each domain has a source
- Source = Authority Document
- E.g. PCI comes from the PCI Council, which puts out the Data Security Standard (the latest version is PCI DSS 3.0)
- E.g. Healthcare comes from Congress, which puts out 3 laws: HIPAA, HIPAA Electronic Health Record Technology, HITECH title within the American Recovery and Reinvestment Act of 2009; the Code of Federal Regulation 45 Part 164; and 2 National Institute of Standards of Technology (800-53 revision 4 and 800-66). All of these combine for 6 Authority Documents.

Coalfire

Mapping Controls

The process for control mapping:

- Mapping requires determining if the control is applicable or not
- This process can take between 40-120 hours
- Consider Top Down versus Bottom Up mapping
- Mapping identifies the business units' responsibilities
- Note that some domains are more prescriptive than others
- Mapping creates heightened awareness of where the controls originate
- Allocate at least 3 months to complete this task

Coalfire

Aligning the Examination Windows

What can affect the examination window:

- Some audits cover a period of time, others a point in time
- Filing dates could restrict when the audit is performed
- Evidence goes stale after ~3 months
- Some domains won't correspond with other domains, expect duplication LOE
- Credentials for auditing each area can impact the efficiency

Coalfire

Identifying Audit Overlaps & Sequencing Audits

The process for identifying audit overlaps/ sequencing audits:

- Understand dependency with 3rd parties
- With data in hand, begin the audit planning process
- Sequence the audits and send the schedule in advance
- Ensure data provided during audit can be stored centrally and shared
- Conduct a Post Mortem analysis after each audit
- Continuously update and improve

Coalfire

Benefits and Building a Business Case

CONSOLIDATED AUDIT PROGRAM

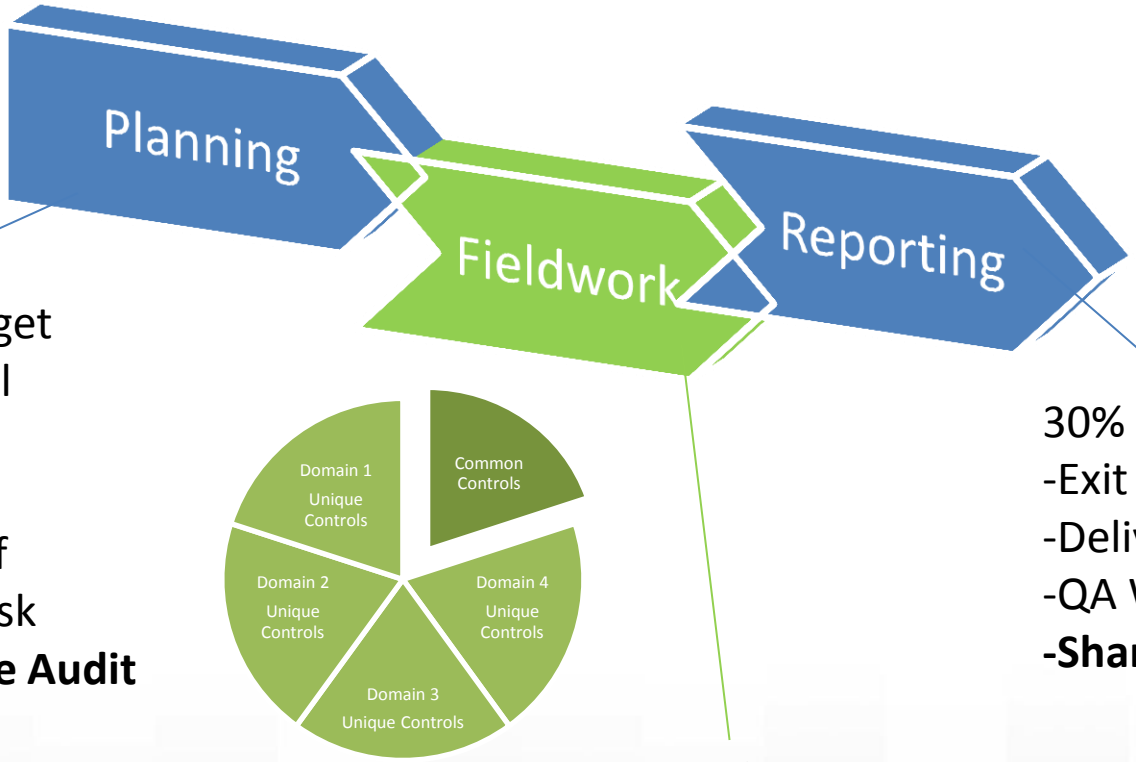
Coalfire

Reduce Cost

- **Streamline audit to orchestrate efficiencies**
  - Know precisely the # of controls
  - Build a budget estimate. Hours per control * # of controls = Total Cost
- **Optimize your time and reduce audit exhaustion**
  - Rule of thumb is: every audit 1 creates 5 hours of internal work for the client
  - Minimize audit season from “year round” to 1-2 month window
  - Stop testing controls that do not mitigate sufficient risk
  - Eliminate need to refresh controls using a manual process (30-90 hours)
- **Empower the business to stay focused on core mission**
- **Organize the process and avoid wasteful spending**

Coalfire

Why it isn't just about reducing fees…

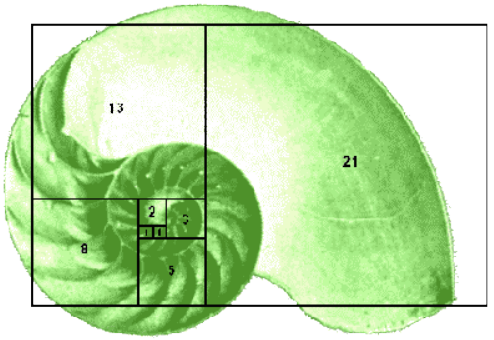


30% of Budget
-Charter Call
-RFI
-Audit Plan
-Assign Staff
-Evaluate Risk
-Orchestrate Audit

40% of Budget
-Interview staff
-Collect Samples
-Control Mapping
-Onsite Testing
-Rely on common controls

30% of Budget
-Exit Meeting
-Deliverable
-QA Work
-Share "common" report

Order Matters



Determining which type to perform first:

- ISO cannot rely on other types and cannot share information
- Double overlap audits may happen when you introduce ISO
- PCI requires QSA test controls
- HIPAA and SOC can rely on other controls (can usually go last)
- Federal will have its own idiosyncrasies
- Examination windows and sample sizes can vary between domains

Coalfire

CAP as a Solution

Why CAP is beneficial:

- Save the client time (x people * hours per audit * # of audits)
- Reduce audit exhaustion
- Use a framework that updates quarterly, like the UCF
- Track higher risk controls more closely (common controls)
- Focus on improving the audit process:
  - Coordination up front
  - Orchestrating an efficient audit
  - Socialize findings and help them through each step
  - One auditor to hold accountable
  - Showcase our expertise in each area and why it makes us unique

Coalfire

Challenges for Service Providers w/ PCI

- New technology changes the compliance landscape
- New and often times conflicting requirements between standards
  - PCI DSS 3.0 – Service Providers
  - PCI DSS3.0 – Self Assessment Questionnaire (SAQ) – A/B/C/D
  - PCI DSS 3.1 – ROC (NEW)
- Virtualization and cloud services
- Mobile devices and new methods of payments
- PCI 3.1 introduces additional responsibility with these controls:
  - 8.5.1 Additional requirement for service providers: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.
  - 12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.
  - 12.9 Additional requirement for service providers: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

Coalfire

Challenges for Service Providers w/ Federal

- New and often times conflicting requirements between standards
  - NIST SP 800-53 Revision 3 to Revision 4 transition
    - Relocated, removed and consolidated controls—which to follow?
  - Addition of draft baseline for FedRAMP High Impact system level
    - Uplift from Agency required controls under FISMA to FedRAMP
  - Continuous monitoring impacts?
    - Weekly, monthly updates from the traditional quarterly updates
  - Use of VMware, and other cloud solutions, changes architecture

Coalfire

Challenges for healthcare compliance

- New technology changes the compliance landscape
  - Wearable devices
  - Wireless devices in the room
  - Digital records available for download
  - Mobile apps taking on more healthcare functionality

- New and often times conflicting standards
  - HIPAA and/or HITRUST
  - Overlap with Other Domains?
  - Merging frameworks in the works
  - Use of VMware, and other cloud solutions, changes architecture

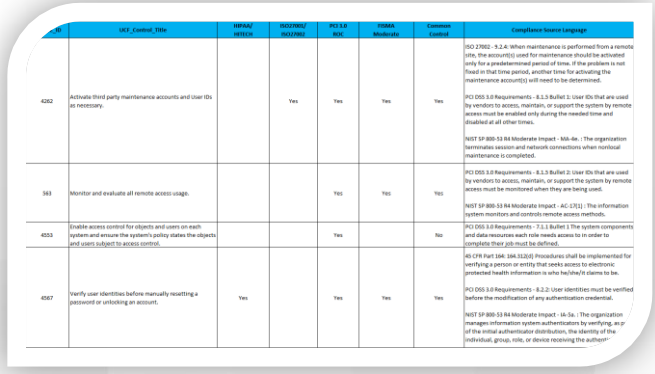
Goalfire

Customizing a solution to meet your needs

- Path to completeness and accuracy begins with controls
  - How many controls does HIPAA introduce?
  - How much overlap do you have with other domains?
- UCF tool has identified 28 regulatory standards under Healthcare and Life Sciences. CFS narrows this to…

Regulatory Body / Standard Name
21 CFR Part 11
21 CFR Part 820
42 CFR Part 3 Patient Safety and Quality Improvements
42 CFR Parts 412, 413, 422 et al.
45 CFR Part 160
45 CFR Part 164
CMS Core Security Requirements CSR
CMS Information Security Risk Assessment IS RA Procedure
CMS Information Security Terms Definitions
CMS Records Schedule
CMS System Security Plan Procedure
Department of Health and Human Services Records Management Procedures Manual
European Commission
European Medicines Agency
FDA General Principles of Software Validation
FDA Guidance for Industry Part 11 Electronic Records and Signatures
Good Practices For Computerized systems In Regulated GXP Environments
HHS Records Management Handbook Appendix B - General Records Schedule
HIPAA
HIPAA Electronic Health Record Technology
HIPAA HCFA
HITECH title within the American Recovery and Reinvestment Act of 2009
HIPAA Electronic Health Record Technology
HITECH title within the American Recovery and Reinvestment Act of 200
The Patient Safety and Quality Improvement Act of 2005
URAC
US Centers for Medicare and Medicaid Services
US Congress
NIST SP 800 66
NIST SP 800 53 R4

170 HIPAA controls



Coalfire

Questions?

Coalfire

Unified Compliance Framework (UCF) Definition and Demo

PART TWO

Coalfire

Unified Compliance Framework (UCF)

UCF was developed to answer the following questions:

- Can the organization's existing controls be used for attestation under multiple regulatory initiatives?
- Which regulatory initiatives overlap with others?
- Which regulatory initiatives fill the gaps left by others?

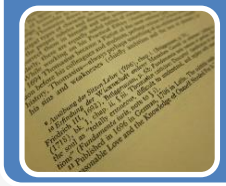
Coalfire

Unified Compliance Framework (UCF)

- **Coalfire is using the UCF as the CAP control library**
  - 30,000+ overlapping citations from 900+ regulation standards, guides, across 38 countries
  - Includes mapping of over 5,000 IT control statements
  - Coalfire has corporate developer license @ $250 per domain license

Authority Documents (AD)

- Updated within 3 months of issuance
- Contains all historical instances & deprecated records
- Coalfire has mapped these to Coalfire audit plans



Citations

- Broken out into smallest control level
- Language from AD included with traceable reference
- 1 citation is mapped to many controls (1:*)

Controls

- Normalizes control based on UCF control language
- Identifies common controls
- Grouped by AD with industry label i.e. Healthcare, PCI

UCF

Understand the compliance food chain

- **The UCF is a legal framework**
  - Every control must be mapped to the source document
  - There is no “tool” -- just an Excel Spreadsheet and SQL scripts
  - Every analysis is a manual process; scoping takes 2-3 hours alone
- **Every organization is different**
- **Process enables you to jump-start the process**
  - Confirm all of the domains
  - Easily add or remove domains
  - Understand the context for the controls

Coalfire

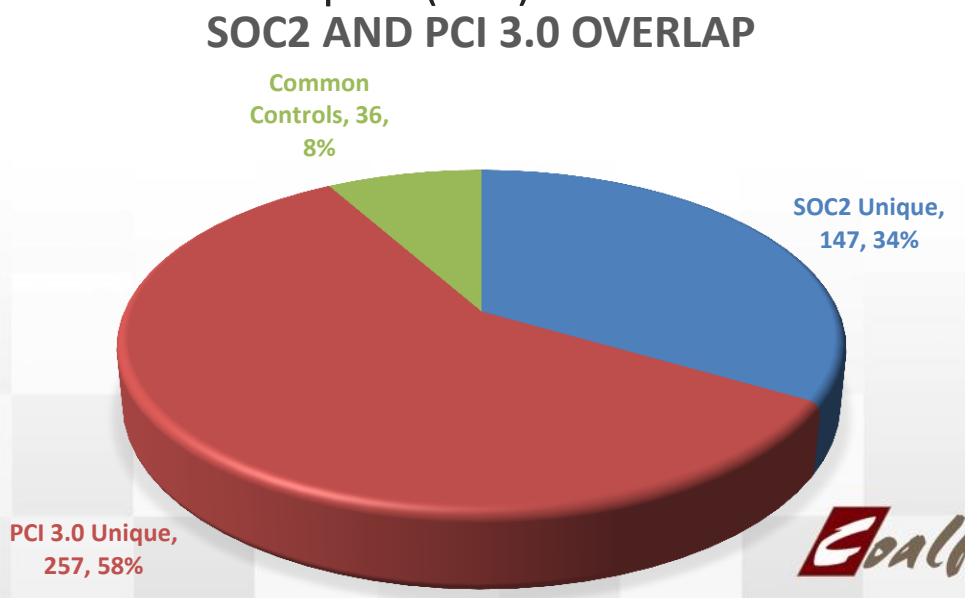
The Science of Compliance®

DEMO

Coalfire

Example: PCI 3.0 and SOC 2 Overlap

- **PCI 3.0 and AT101 (AICPA standard used by SOC2)**
  - How many controls overlap?
  - What's the incremental cost?
- **SOC2**
  - Cloud Security Alliance (CSA) framework
  - Depends on which of 5 Trust Service Principles (TSP)
    - ✓ Common Criteria / Security
    - ✓ Availability
    - ✓ Confidentiality
    - ✓ Information Processing
    - ✓ Privacy



Reduce Risk

- **UCF tool provides a common control ID and language**
  - Easier to identify control overlaps
  - Highlight the common controls and emphasize dependency
  - External auditor can leverage the same language tool (no cross walking)
- **UCF reference of the citation can let you:**
  - Trace the control with legal language
  - Allow control owners to understand the story
- **UCF metadata includes:**
  - Control Owner
  - Association of a control with an asset
  - Ability to enter audit procedures
- **Focus on embedding the controls into organization, not mapping**

Sample Work Product

WALKTHROUGH

Coalfire

Carlos Peláez
Director, Coalfire
877.224.8077 ext. 7079
Carlos.Pelaez@coalfire.com
www.coalfire.com

Craig Isaacs
CEO, Unified Compliance
510.962.5192
cisaacs@unifiedcompliance.com
www.unifiedcompliance.com

Coalfire®

UCF

Coalfire Whitepapers:

Whitepaper - FedRAMP and FISMA: Controls and Authorization Differences

VMware *VCE* Product Applicability Guide for Compliance with HIPAA

VMware FedRAMP Architecture Design Guide

VMware PCI 3.0 Architecture Design Guide

Other Interesting Links:

Largest Data Breaches

Federal Cybersecurity Breaches Mount Despite Increased Spending

ISO: Trust and confidence in cloud privacy

HITRUST-AICPA Advisory Panel & Working Group

SANS Healthcare Cyberthreat Report

Coalfire