CSA presents SECtember 2022

CSA cloud security alliance®

Continuous Monitoring

Design, Automation, and Implementation in the Cloud

PRESENTED BY

weaver
Assurance • Tax • Advisory

Eric Peeters
Senior Manager

About Me

Eric Peeters

Senior Manager, IT Advisory

eric.peeters@weaver.com

817-882-7395

TCU Frog and Big 12 Orphan

Solving problems by drinking coffee

Living in the clouds most days

15 years in IT Ops and Audits

Cloud Services @ Weaver

About Weaver

Services & Industries

Services

Assurance

- Agreed-upon procedures
- Audit, review & compilation
- Employee benefit plan audit
- IFRS assessment & conversion
- Peer review services
- SOC reporting services

Tax

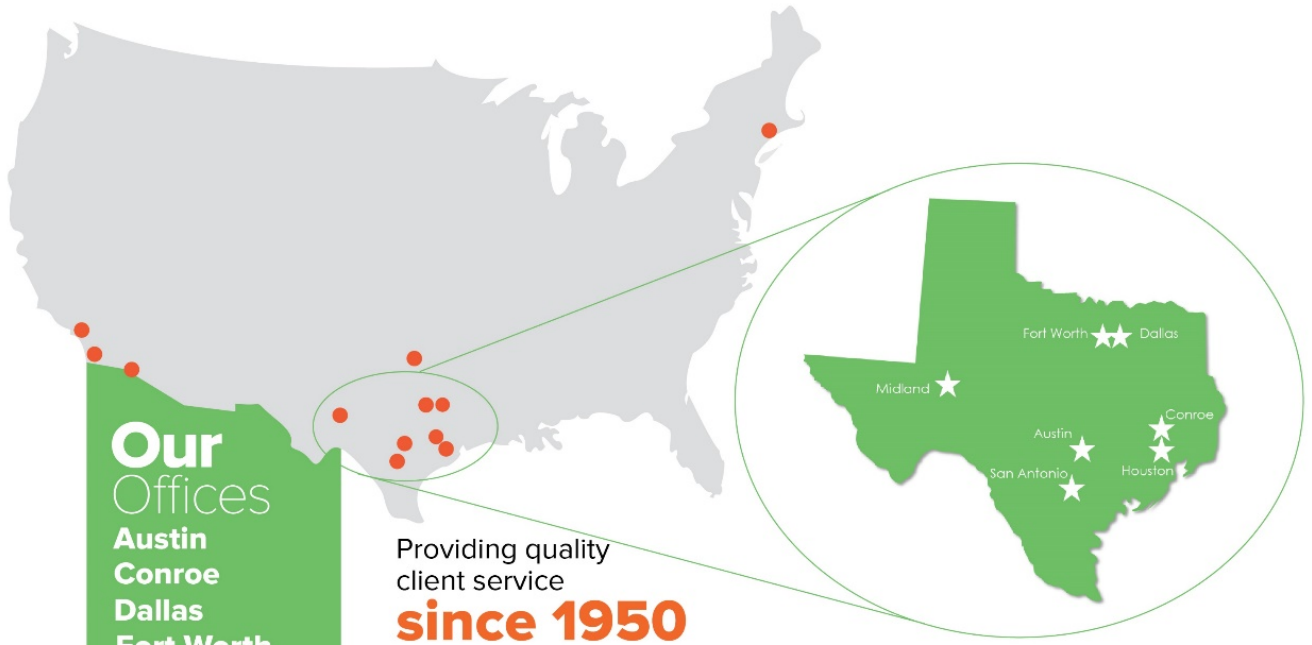
- Federal tax
- International tax
- State & local tax
- Private client services

Advisory

- Energy compliance services
- Forensics & litigation services
- Public company services
- IT advisory services
- Risk advisory services
- Transaction advisory services

Industries

- Energy
- Financial services
- Manufacturing & distribution
- Construction
- Technology
- Real estate
- Public sector
- Health care



Our Offices

Austin
Conroe
Dallas
Fort Worth
Houston
Los Angeles
Midland
New York City
Oklahoma City
San Antonio
San Diego
Woodland Hills

Providing quality client service **since 1950**

12 U.S. locations

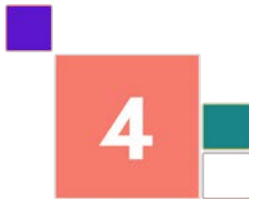
Largest independent accounting firm based in the **Southwest**

Agenda

What is a Continuous Monitoring Program

Designing a Continuous Monitoring Program

Deploying Automation as Part of the Program

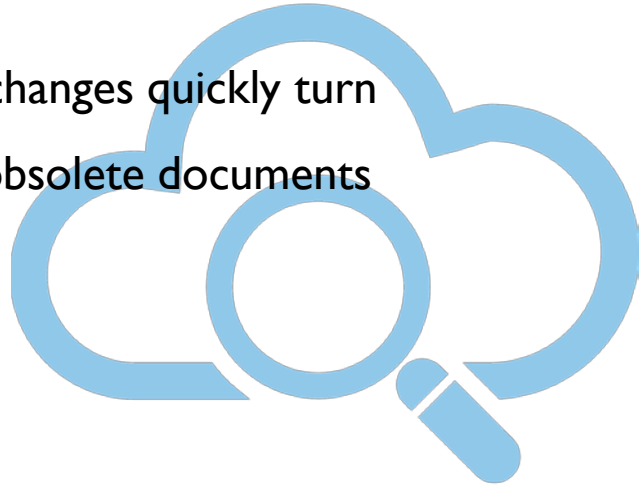


Considering Insourcing vs Outsoaring the Program

Why Continuous Monitoring in the Cloud

In the Cloud

- More integrations means more third-party risks
- Ephemeral services hard to measure and audit
- Fast-paced technology changes quickly turn historical reports into obsolete documents



Why Continuous Monitoring

- Extended period to plan remediation
- Visibility into the health of critical suppliers
- Risk assessment over key components
- Enhanced monitoring of less mature systems
- Update to outdated ISO/SOC reports
- Continuous demonstration of compliance

Defining Continuous Monitoring

It Is Not (Only)

- Real-time, 24/7, non-stop monitoring
- Replacement for traditional compliance audits
- Automated controls monitoring

It is

A set of procedures or activities that facilitate **rapid detection** of process deviation from policies, standards, or internal and external commitments over the technology environment

Rapid Detection is defined by each entity on a process-by-process basis based on a combination of commitments, constraints, risk appetite, and capabilities

Steps to a ConMon Program

Goal

Key step in the definition of Scope and Findings Review

Scope

Scope is based off Goal and Objectives of the ConMon

Findings Review

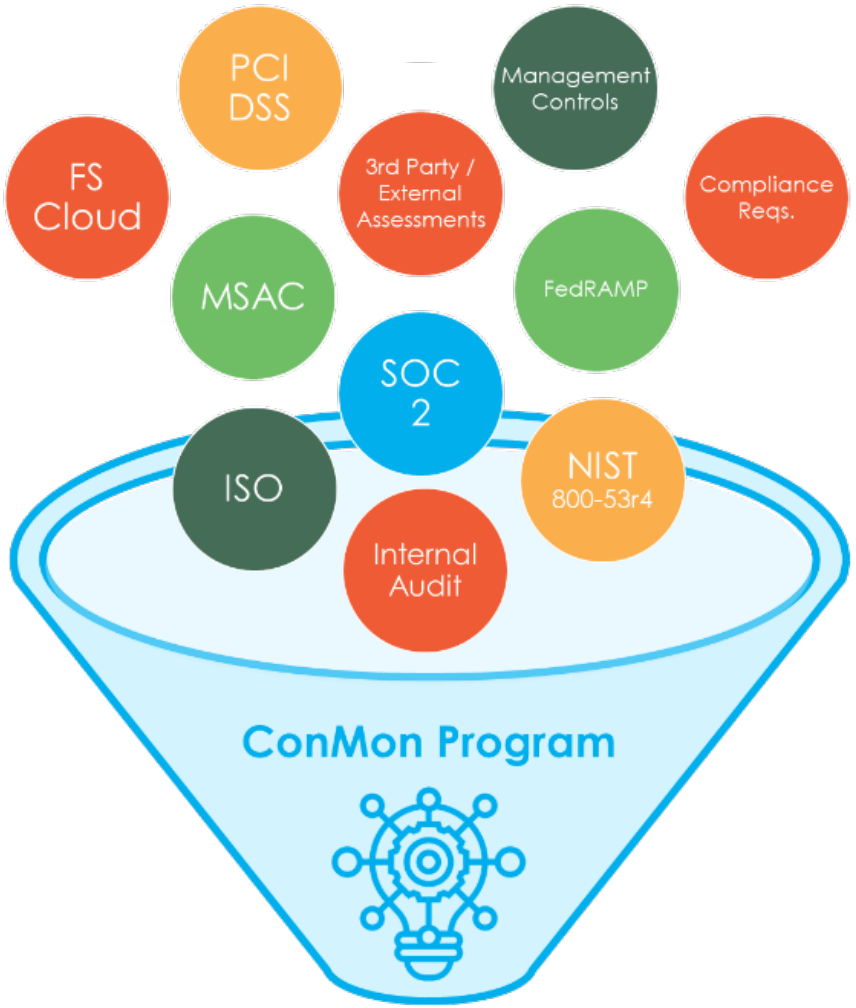
A ConMon program is nothing without a solid findings review

Objectives

A ConMon program may have multiple objectives

Procedures

Heavily dependent on scope and objectives



Goal: Why Are We Doing a ConMon

Demonstrate Compliance

External requirements

Contracts, customer commitments, regulations, etc.

Internal requirements

Policies, risk assessments, standards, etc.

Well-defined compliance metrics

Perform a Health Assessment

Before internal / external audit

Monitor key components of the system

Extended readiness before first compliance audit

Objectives: Pick a Number From 1 to 4

Risk Reduction

Reducing the probability, impact, or both, of failure

Prioritize systems with high risk reduction potential

Early Detection

Identifying deviation before audits and examinations

Advance notice to plan remediation or mitigation

Cost Savings

Cost avoidance: penalties for non-conformance

Cost reduction: automation or higher efficiency

Process Improvements

Tangible benefits: better metrics, faster improvements

Intangible benefits: better communication

Health Assessment scope is flexible and can change frequently based on assessed risk, time-to-remediation or other factors

Scope: Goal + Objectives

Compliance Goal

Minimum scope = systems with direct influence on compliance

Additions to scope

- Indirect influence and high impact
- Likely candidate for automation
- High cost of non-compliance

Health Assessment Goal

Minimum scope = key components or scope of next audit

ISO, PCI, SOC, etc. may drive scope

Extended readiness before first compliance audit

Procedures: How To Execute A ConMon

1

Design highly repeatable and portable procedures

- Minimal changes when tool or process changes
- Useable through multiple iterations of the ConMon

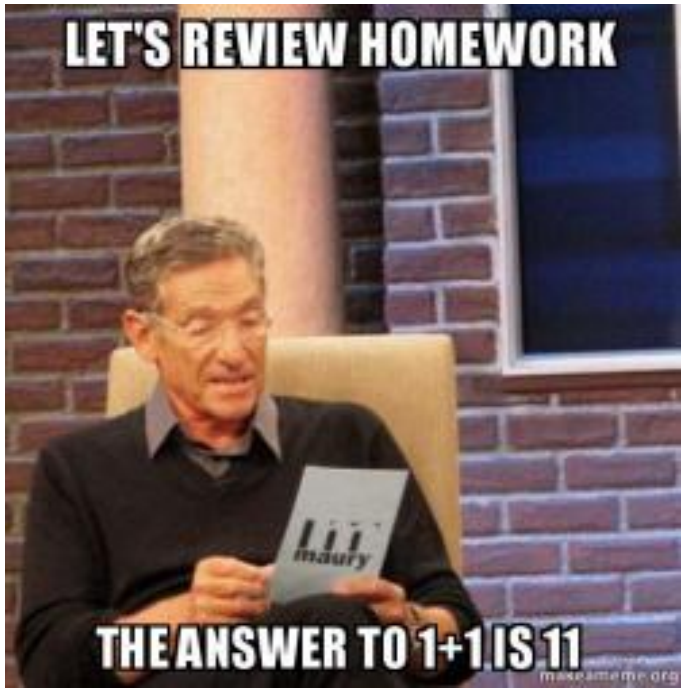
Use Inspection procedures whenever possible

2

Execute, adapt, innovate

- ConMon is not defined by adherence to a controls set or framework
- Update procedures on the fly to meet goal, objectives, collect actionable information
- Document the rational of all changes for future reference

Findings Review: What To Do With It



Keys To A Successful Review

- Deep understanding of goals, objectives of the ConMon
- Also of relevant compliance programs (SOC, PCI, ISO, etc.)
- Root-cause analysis of findings
- Comprehensive remediation and mitigation plans

It's Not The Finding, But The Follow-Up

- Test mitigation and remediation during current or next ConMon
- Prepare process recommendations whenever applicable
- Review scope and procedures considering the findings and maturity of tested components

Continuous Monitoring Tools

Spreadsheets and Macros

Excel functions, macros, pivot tables, and charts

Cheap and easy to get started

Cloud Provider's Tools

Already available

Integrated with other resources

Limited features

Weak reporting capabilities

Third Party Tools

Wide choice of features

Multiple cloud integrations

Definition of needs and capabilities crucial

Selecting a Third-Party Monitoring Tool

Other Considerations

- It will take longer than advertised!
- Plan on multiple iterations to fine-tune data collection and analysis
- Talk to your third-party auditors
- It will take longer than promised!

Capabilities Alignment

Map needs to the right tool:

- Documentation workflow management
- Policy management and enforcement
- Agent-based or agentless data collection, analysis, and reporting
- AI / ML driven analysis

Consider future compliance needs

Validate availability of data for analysis

- Data sharing vs compliance with internal policies
- Capability and compatibility of existing systems

Planning For Implementation

Identify ConMon procedures to be automated

- Highly repeatable and systematically executed
- Artifacts uniformly created and uniquely identifiable from similar but unrelated artifacts

Prepare Validation Plans

- Testing required to validate the accuracy and completeness of automation
- Document configuration, data sources and data paths – review upon every change

Plan For Alerts And Failures

- Threshold and destination of alerts
- Responsibilities for responding to alerts
- Alerts to detect automation failure: unusually low activity threshold, daily activity report, etc

Considerations for Insourcing vs Outsourcing ConMon

Insourcing

Pro

- Lower direct program costs
- In-house expertise over processes and technology
- Faster response time to changes in need

Con

- Personnel with multiple competing responsibilities
- No formal training in compliance standards
- Limited experience in designing procedures

Outsourcing

Pro

- Experienced in procedures design and assessment
- Ongoing training in compliance standards
- Bench of additional expertise available as needed

Con

- Higher direct program costs
- Lack of institutional knowledge
- Limited availability outside of planned timeframe

Key Takeaways

Plan for ConMon first

Plan for Automation next

Scope and Review are keys to success

Fully understand Automation options

weaver
Assurance • Tax • Advisory

Eric Peeters, Senior Manager, Cloud Services

eric.peeters@weaver.com

817 882 7395

https://www.weaver.com/

https://www.linkedin.com/in/peeterse/

CSA presents

SECtember℠

Changing the way the cloud and cybersecurity industry meets