Parallel Track 4 - Day 1

Hosted By: **Scott Schwan**, Co-Founder and CEO, *Shujinko*
Rick Harwood, VP of Engineering, *Shujinko*

(OSCAL Webpage)

Bring your coffee or lunch

and join us at **1:45 PM**

NIST | FedRAMP

NIST: oscal2021@nist.gov
FedRamp: info@fedramp.gov

SHUJINKO

Leveraging Compliance Automation

For a Cloud-First World

Introduction

Scott Schwan

Co-founder & CEO of Shujinko

Mr. Scott Schwan is a co-founder and serves as Chief Executive Officer at Shujinko. Previously Scott was the director of cloud engineering at Starbucks, where he led a team of talented DevSecOps engineers practicing infrastructure and security-as-code to build a shared platform for Starbucks development teams. Prior to Starbucks, Scott was a technical leader at CardFree, Tommy Bahama, PricewaterhouseCoopers, and SAP. He has a background in security and infrastructure engineering that is heavily focused on IT compliance, retail, e-commerce, mobile order and pay (MOP), and loyalty.

Introduction

Rick Harwood

VP of Engineering at Shujinko

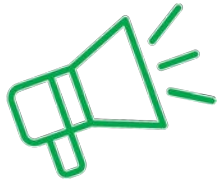
Mr. Rick Harwood is the VP of Engineering at Shujinko where he is responsible for building innovative software products that simplify, automate, and modernize the management of IT audits. Prior to joining Shujinko, Rick held engineering executive positions at Starbucks where he led some of the most innovative and critical software engineering teams for 8 years. Prior to Starbucks, Rick held a leadership role at the startup Blue Gecko, and software developer/engineering roles at both Amazon and Oracle. Rick hails from Tennessee and attended UW for his bachelor's degree.

Overview

Digital Transformation

Compliance Automation

Current Patterns



OSCAL in Use Today

Questions

The Why of Digital Transformation

- Per Forrester/Accenture, the three main drivers for digital transformation are:
  - Profitability
  - Customer Satisfaction
  - Increased Speed to Market

- “An effective digital transformation program is aware of its interconnectedness with everything within the business.”
  - MIT/Capgemini

Digital Transformation in the News

- “Starbucks to step up rollout of 'digital flywheel' strategy”
- “Capital One to Shut Down Its Last Three Data Centers Next Year”
- “Microsoft Analysts: Q1 Shows Payoff From Cloud Shift, Azure Narrowing The Gap With AWS”
- “Taco Bell's new mobile app the brand's 'biggest innovation since the drive-thru'”

Cloud First - Impacts to Security and Compliance

10 Years Ago

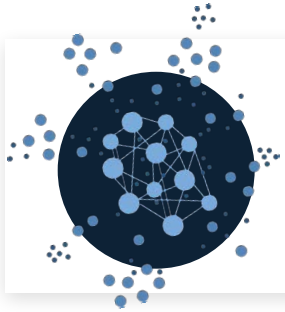
IT
In-House

Apps
Monolithic; Predictable, infrequent Releases

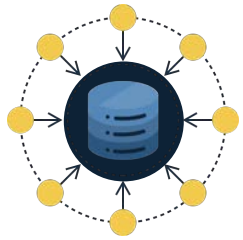
Data
Centralized; Finite sources and size

Today

IT
Cloud: Azure, AWS, GCP, in-house



Apps
Microservices, Changing Daily



Data
Number of Sources; Size & Growth
3rd Party SaaS Tools

Definition - Compliance Automation

- If we reference both the ISACA glossary and the International Society of Automation (ISA) glossary we get the following:

- Compliance Automation

    - The creation and application of technology to monitor and control the adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies.

Don’t Automate for Automation’s Sake

Too Much Time

- ➔ Manual, labor-intensive, dreaded
- ➔ Tons of back and forth

Mess of Tools

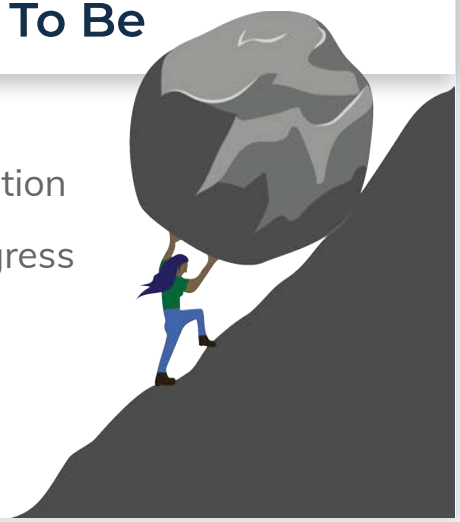
- ➔ Spreadsheets
- ➔ Email, Gdocs, Slack

Compliance Testing

Unclear Communication

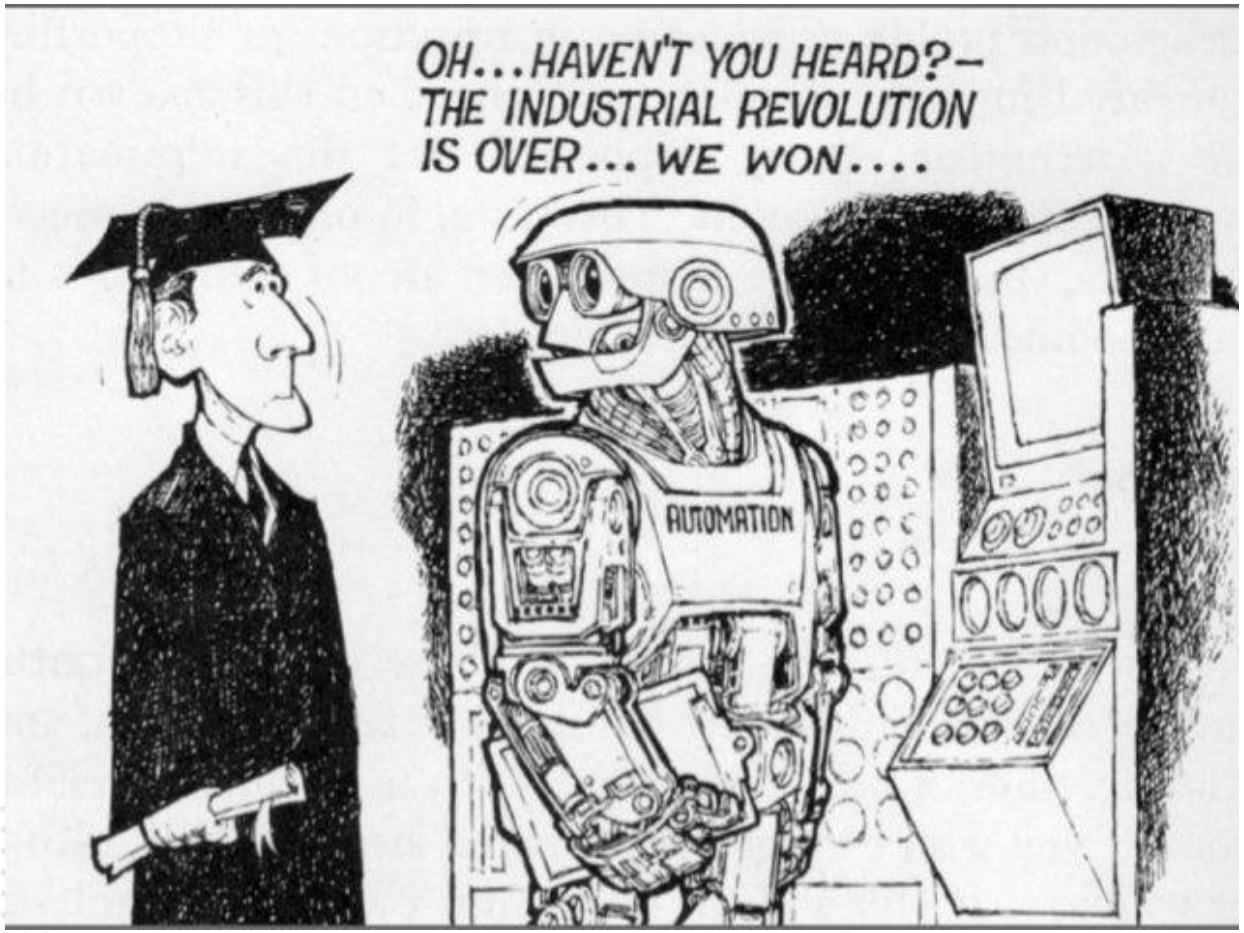
- ➔ Engineers are saying:
  - ◆ “What are you asking for?”
  - ◆ Screenshots, organize?
  - ◆ “I HATE this!”

Harder Than It Needs To Be



- ➔ Evidence collection & collaboration
- ➔ Hard to gauge status and progress

Dispelling the 100% Automation Myth



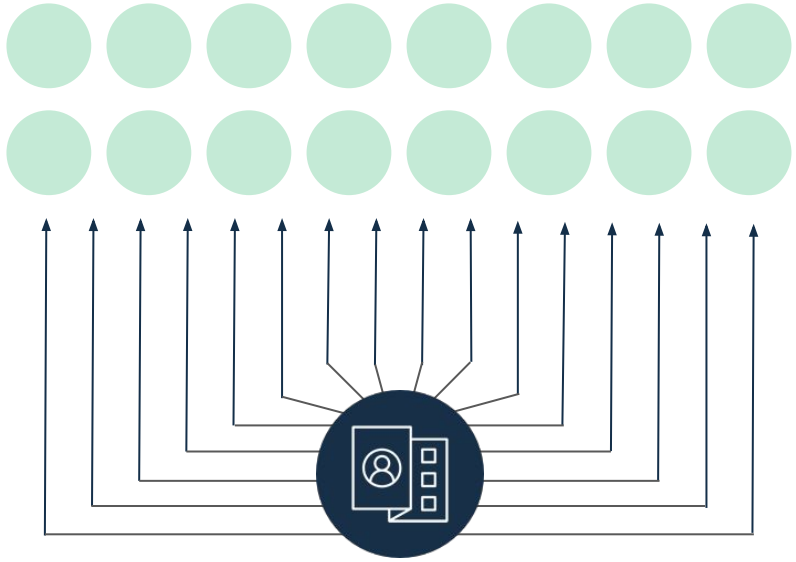
Compliance Automation - Current Patterns

- Complexity is based upon the automation maturity of an organization
- Patterns are augmenting, not replacing IS audit, control, and security professionals
- Amazingly enough, the engineers you are requesting the evidence from are more than happy to automate themselves out of manual evidence collection
- Prioritize your automation efforts to focus upon the biggest time savers

Pattern - Evidence Requests

✕ Manual

Control and System Owners

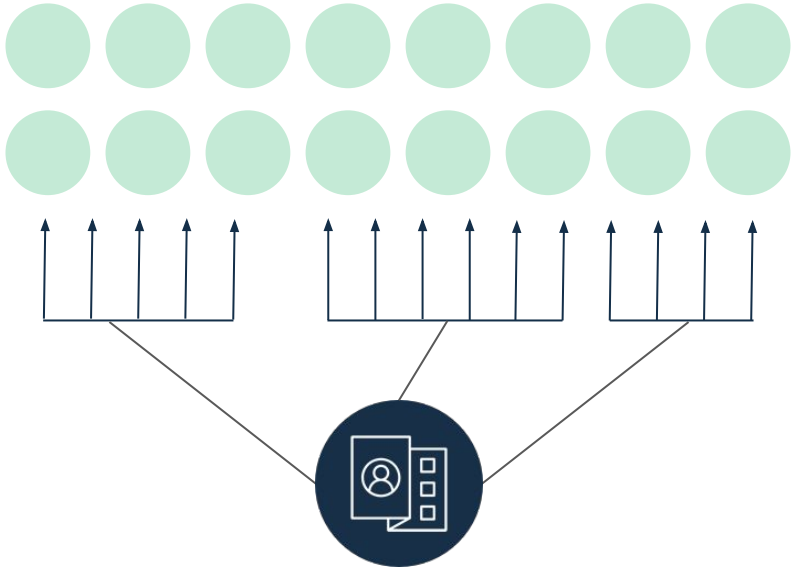


Evidence Request Emails, Messages, Task Assignment

Audit Document Request List: 200+

✓ Automated

Control and System Owners



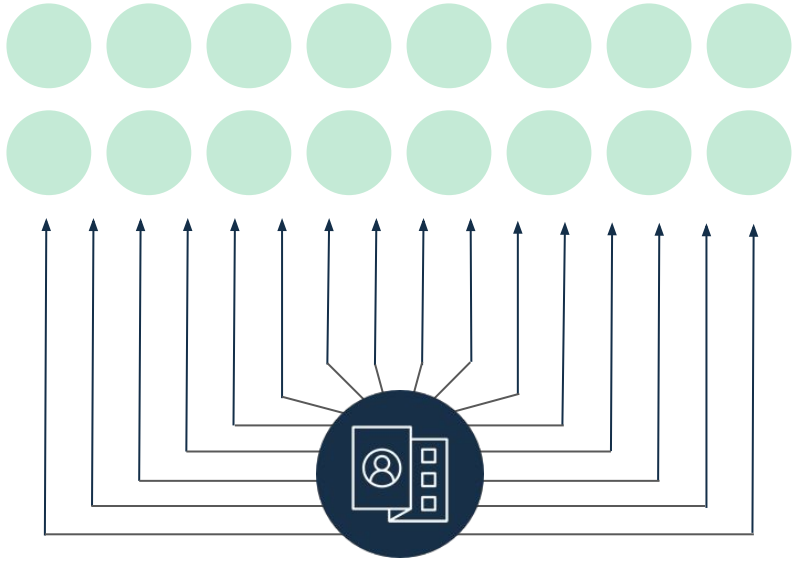
Scheduled Evidence Requests Sent in Accordance with Testing Frequency

Bulk Requests: 1 Daily, 1 Weekly, 1 Monthly

Pattern - Evidence to Control Mapping

✕ Manual

Controls

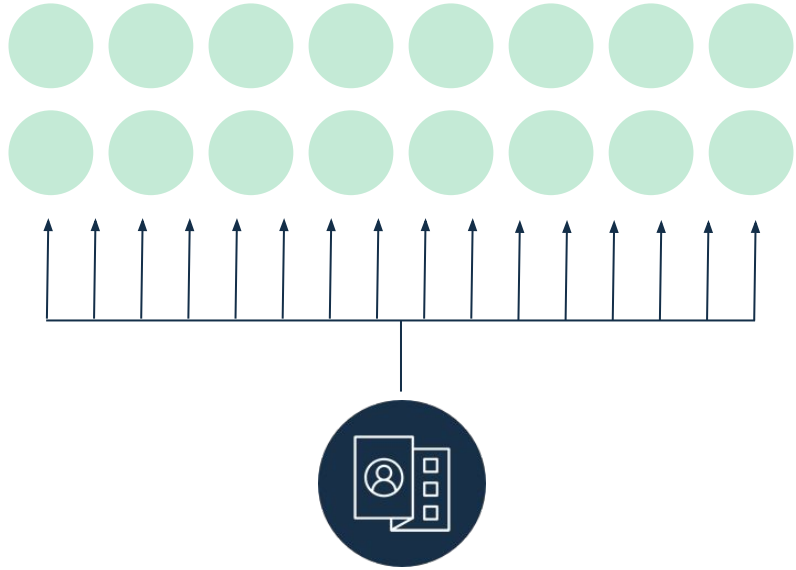


Evidence:
Information Security Policy

23 individual uploads

✓ Automated

Across Controls & Compliance Standards

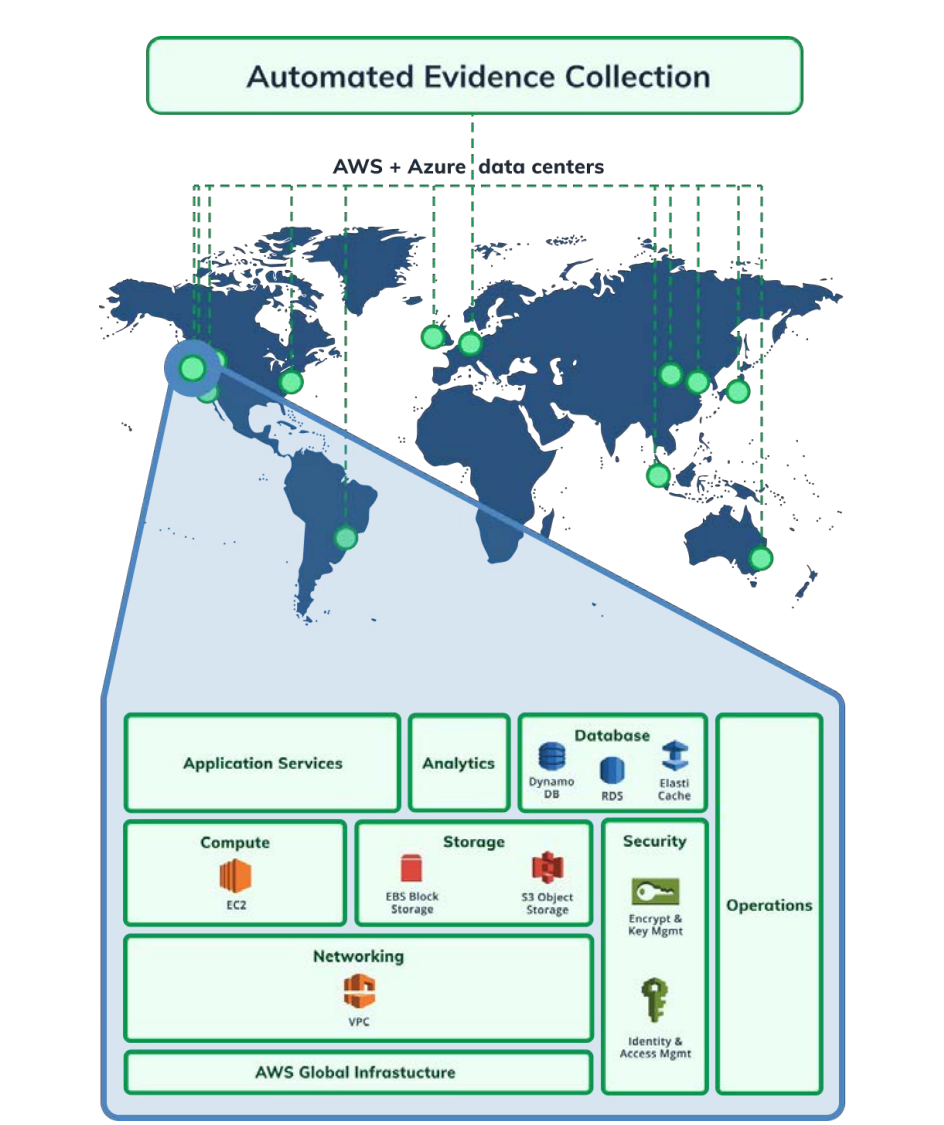


Evidence:
Information Security Policy

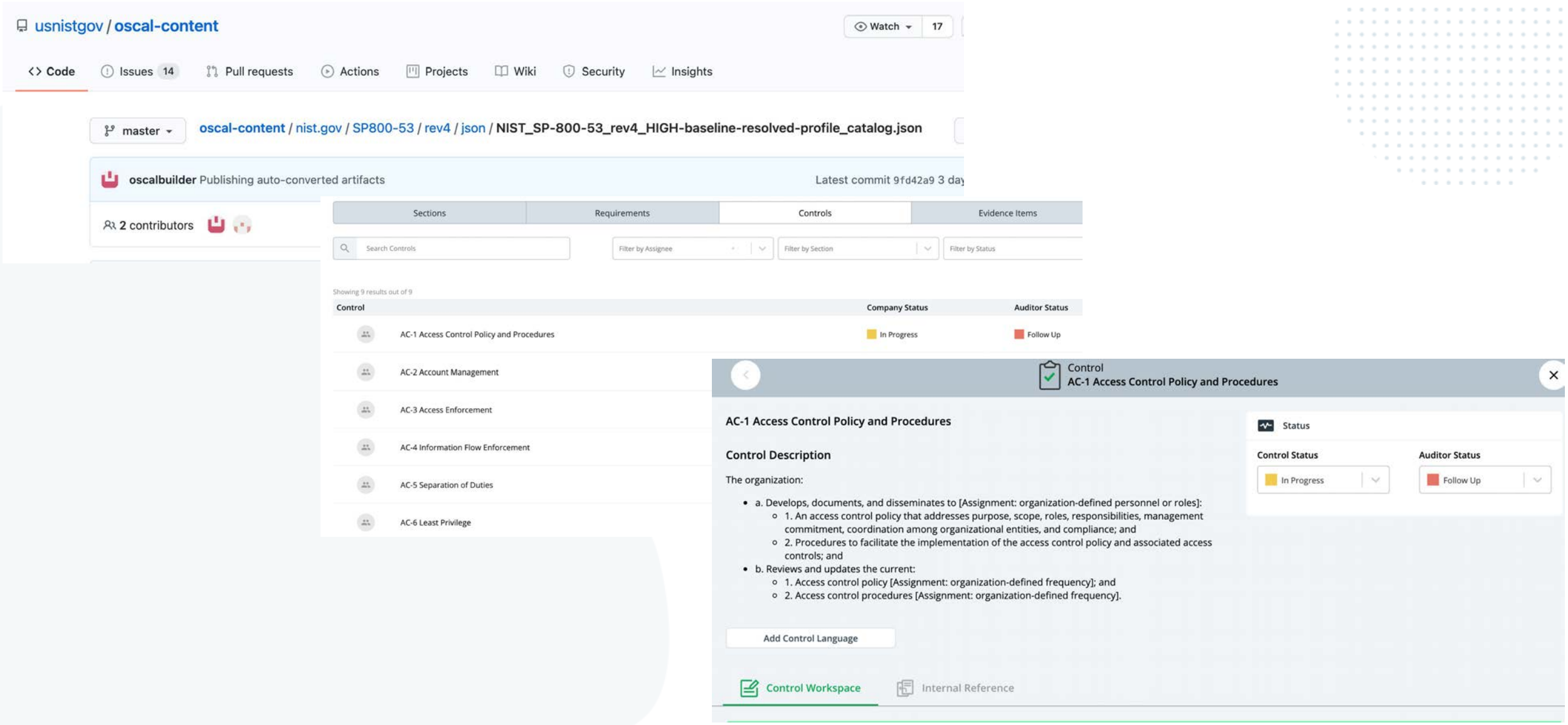
1 automated upload

Pattern - Evidence Collection

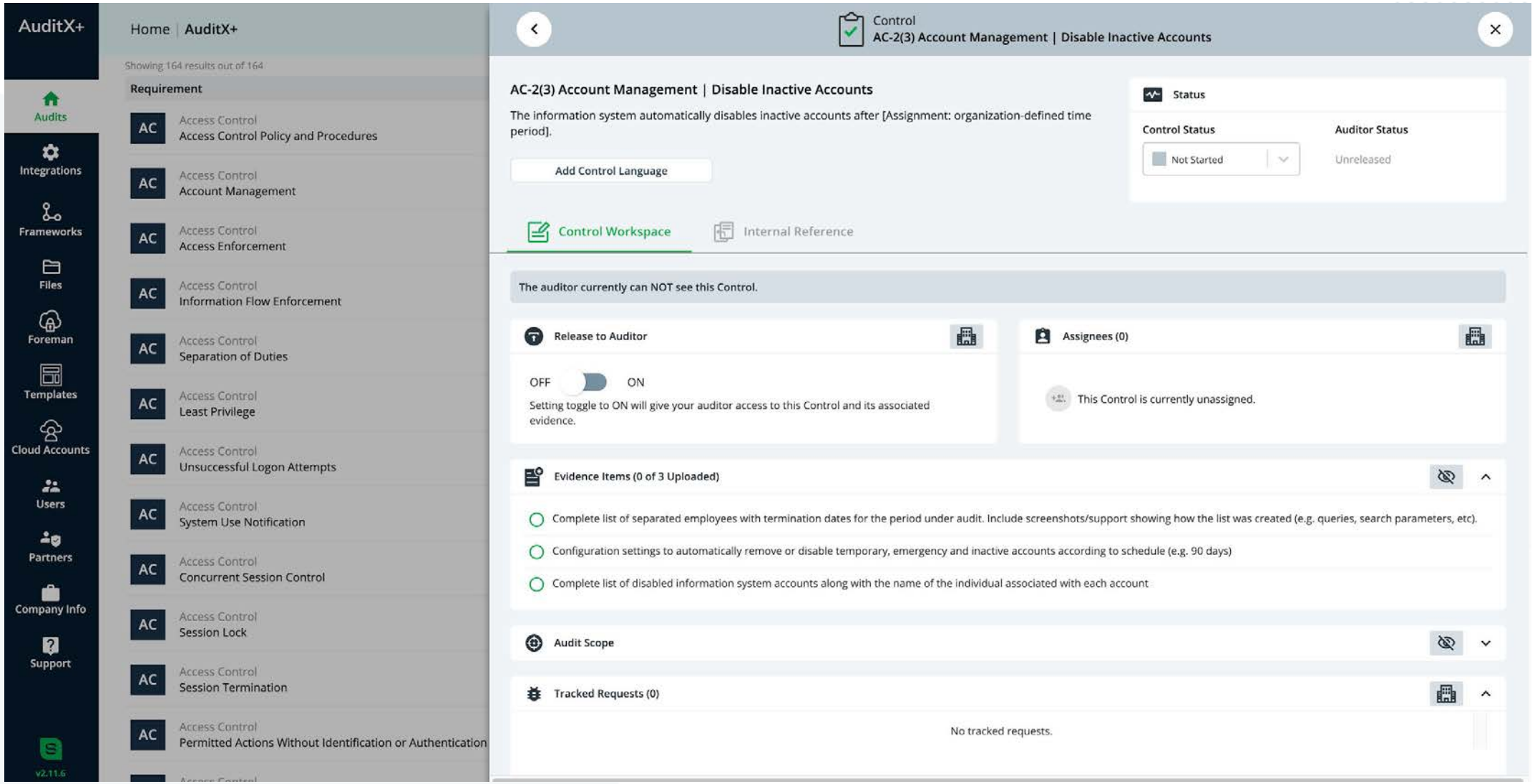
- Everyone hates screenshots
- Scripting repetitive requests for evidence collection saves time during testing, retesting, and additional sampling
- Biggest challenge is putting the output into a format that maps to the spirit of the control language and isn't just a raw dump of data
- Engineer readable doesn't always translate to Auditor readable



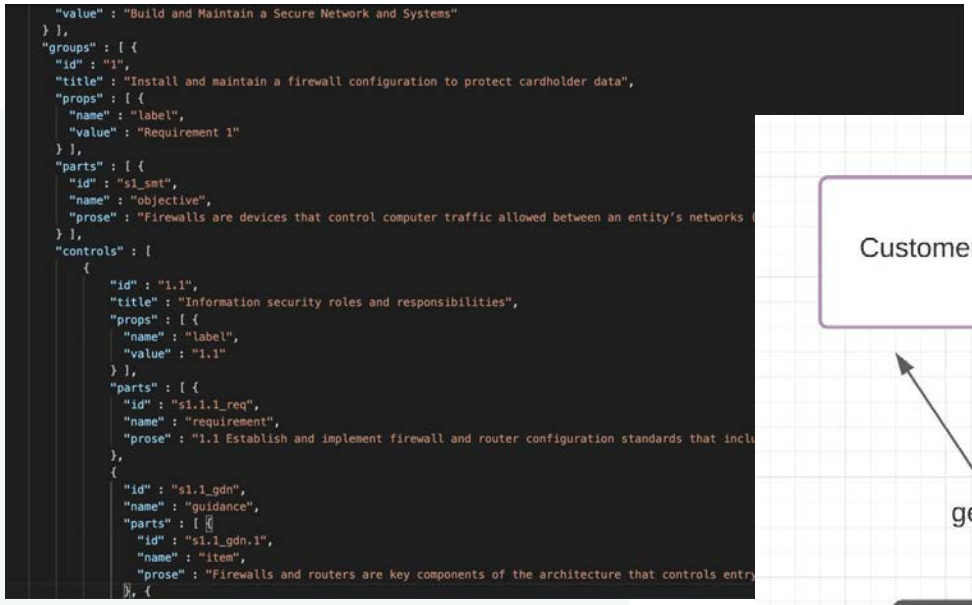
The OSCAL model - initial use case @Shujinko



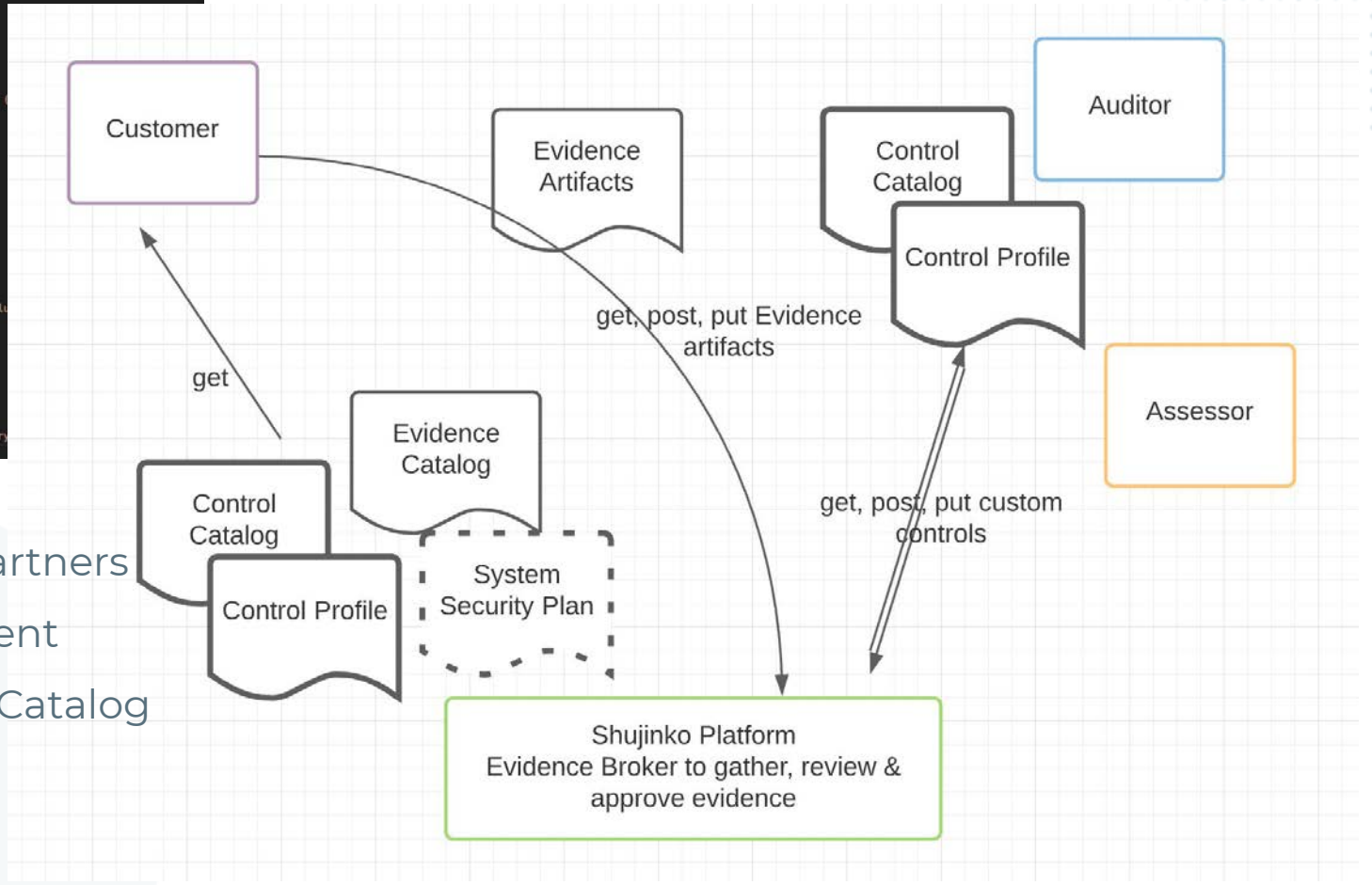
The OSCAL Model - In Software-as-a-Service



The OSCAL model - next use cases @Shujinko



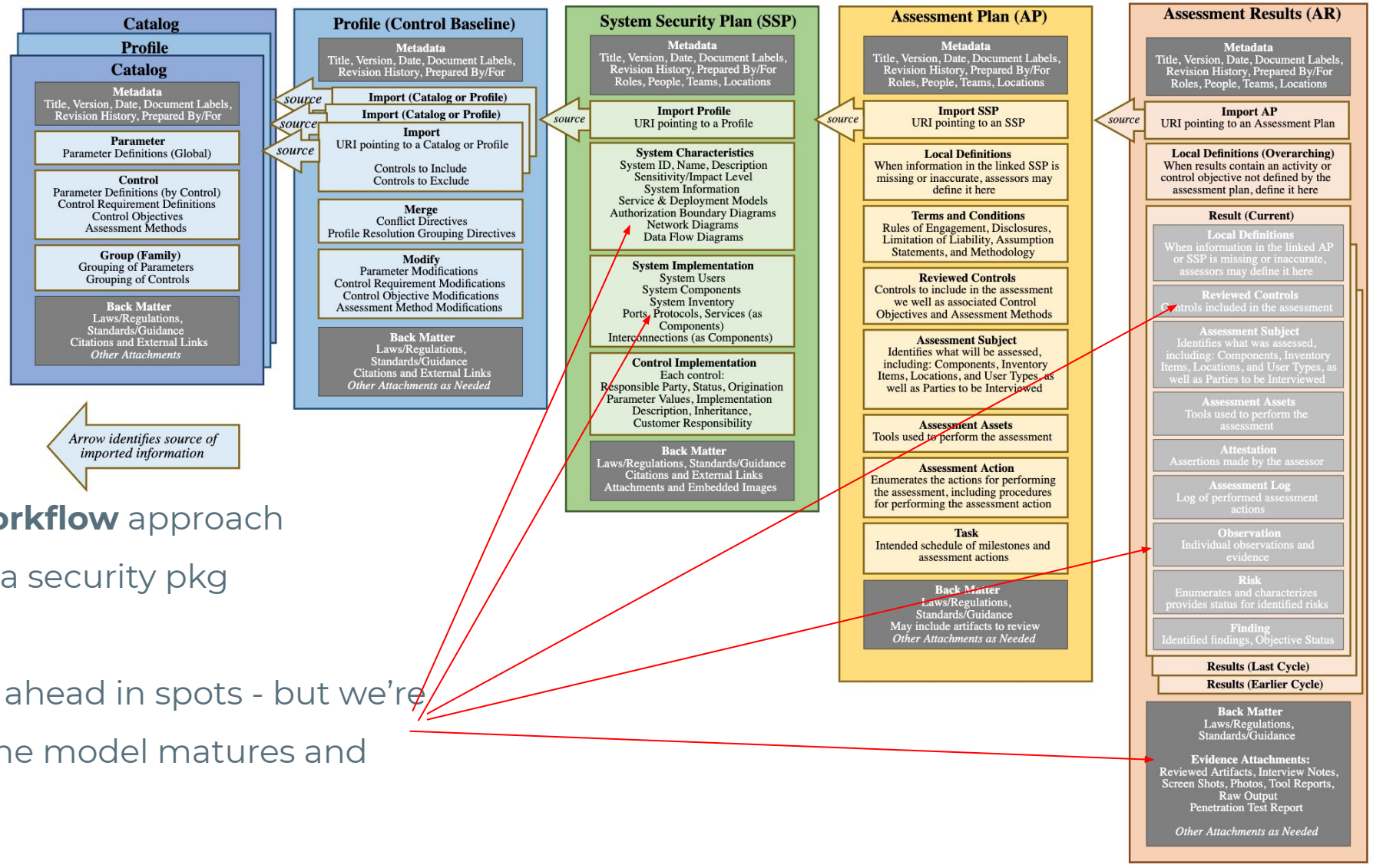
```
    "value" : "Build and Maintain a Secure Network and Systems"
  } ],
  "groups" : [ {
    "id" : "1",
    "title" : "Install and maintain a firewall configuration to protect cardholder data",
    "props" : [ {
      "name" : "label",
      "value" : "Requirement 1"
    } ],
    "parts" : [ {
      "id" : "s1_smt",
      "name" : "objective",
      "prose" : "Firewalls are devices that control computer traffic allowed between an entity's networks
    } ],
    "controls" : [
      {
        "id" : "1.1",
        "title" : "Information security roles and responsibilities",
        "props" : [ {
          "name" : "label",
          "value" : "1.1"
        } ],
        "parts" : [ {
          "id" : "s1.1.1_req",
          "name" : "requirement",
          "prose" : "1.1 Establish and implement firewall and router configuration standards that inclu
        },
        {
          "id" : "s1.1_gdn",
          "name" : "guidance",
          "parts" : [ {
            "id" : "s1.1_gdn.1",
            "name" : "item",
            "prose" : "Firewalls and routers are key components of the architecture that controls entry
          }, {
```



Build API Capabilities for Customers, Partners

- Expose Control Catalog Management
- Push Evidence & Map to Evidence Catalog

The OSCAL model - driving further Automation



Aligned with **continual workflow** approach

- Well beyond creating a security pkg

Being a startup, we've run ahead in spots - but we're excited to incorporate as the model matures and companies adopt

Q&A

Thank You

Automated Audit Preparation

Simplify, Automate, Modernize

SHUJINKO

shujinko.io

Parallel Track 4 - Day 1

Hosted By: **Scott Schwan**, Co-Founder and CEO, *Shujinko*
Rick Harwood, VP of Engineering, *Shujinko*

(OSCAL Webpage)

Please return to the main BlueJeans Event Platform. The next event begins at **2:30 PM**.

NIST | FedRAMP

NIST: oscal2021@nist.gov
FedRamp: info@fedramp.gov

Abstract

- What is driving companies to migrate to the cloud and how will it play out?
  - Slides 6 - 9
- What are the implications for security, compliance, and audits?
  - Slide 11
- What is the right level of automation to increase efficiency in audit prep but not incur additional risk?
  - Slide 15
- Why will automation augment and not replace IS audit, control, and security professionals?
  - Slide 16
- How are compliance automation tools being adopted today?
  - Slide 17 - 21 - Need to update OR replace these
- How does OSCAL's framework enable automated evidence collection and audit prep?
  - New content
- How will standardizing controls in a format that's machine-readable affect vendors of GRC and audit prep tools?
  - New content
- How can OSCAL's framework be incorporated into open APIs in audit prep tools in the future?
  - New content

Call to Action

- Digital Transformation and Cloud First Strategies are here to stay
- There’s been a seismic shift in the way we work
- As IS audit, control, and security professionals, we need to learn the tools available to us and leverage them to keep up with the rate of change
- The Compliance Automation and Compliance Automation Testing space is maturing with new tools every day, we should start learning and becoming experts with these tools so that we can keep up

Adoption of Cloud-First Strategies

- A growing majority of companies are aligning their digital transformation with cloud first strategies
- The public cloud providers have been effective in associating their offerings with the three main drivers of digital transformation
- Reflected in their tremendous year-over-year revenue growth
- A global pandemic didn’t even stall this growth

Our Cloud-First World

Month and Day	File Year Range	Search Results	Keyword(s)
Nov. 16th	2010 - 2015	551 mentions	“Digital Transformation”
Nov. 16th	2015 - 2020	8,750 mentions	“Digital Transformation”
Nov. 16th	2010 - 2015	70 mentions	“Cloud First”
Nov. 16th	2015 - 2020	423 mentions	“Cloud First”

SEC.gov EDGAR

- The new EDGAR advanced search gives you access to the full text of electronic filings since 2001.

Surviving in a Cloud First World

- A Sense of Urgency: Surviving in the Age of Digital by Jonathan Smart

- “The rate of creative destruction is now faster than ever. In 1964, a firm listed on the S&P 500 Index could expect to remain on the index for thirty-three years. By 2016, that tenure had fallen to twenty-four years. By 2027, companies can expect to spend no more than twelve years on the index before they’re replaced.”

Compliance Automation is Poorly Defined

- This seems wrong…
- “Compliance automation, also known as automated compliance, is a category of software applications that use artificial intelligence (AI) features and technology to simplify compliance procedures. These applications provide organizations with workflow capabilities related to compliance, including self-assessments, control analyses, corrective action planning and controls testing….” Blah blah blah
- Let’s fix it…

Definition - Compliance Testing Automation

- If we reference both the ISACA glossary and the International Society of Automation (ISA) glossary we get the following:

- Compliance Testing Automation

    - The creation and application of technology to monitor and control the testing of controls designed to obtain audit evidence on both the effectiveness of the controls and their operation during the audit period

Pattern - CI/CD Pipeline

- Deployments are required to be automated with compliance gates in the pipeline
- Control testing occurs early and often with near real-time feedback
- Compliance reports can be run against code and placed in an evidence repository for review and collection