Virtual Room #2

Hosted By: **Max Aulakh**, Co-Founder, *Ignyte Assurance Platform*

(OSCAL Webpage)

Disclaimer: Portions of the event may be recorded and audience Q&A or comments may be captured. The recorded event may be edited and rebroadcasted or otherwise made publicly available by NIST. By attending this event, you acknowledge and consent to having your conversation recorded.

oscal2022@nist.gov
conferences@nist.gov

OSCAL Components

Ignyte Assurance Platform OSCAL Component Aggregation Techniques

Presented by ignyte™ ASSURANCE PLATFORM

Max Aulakh, MBA, CISSP, CISA, CRISC
Chief Executive Officer I Ignyte Assurance Platform

Speaker

Max Aulakh, MBA, CISSP, PMP, ITIL-F

Ignyte Assurance Platform

Max Aulakh is the managing director at Ignyte Assurance Platform. He started his career in the US Air Force and spent the majority of his time in the Middle East during his enlistment. He brings 15+ years of hands-on working experience from global enterprises on automating risk management and cyber security frameworks. Prior to working with the commercial sector, he focused on automating traditional A&A packages under DITSCAP and DIACAP frameworks. His team was responsible for executing 100+ ATOs on various types of classified and unclassified government networks.

His work currently focuses on automating the risk management framework through the use of language analysis for commercial enterprises struggling with cloud and FedRAMP compliance. His experience is formally supplemented by graduate-level education in business with an undergraduate in systems security and computer science from American Military University. Max enjoys cloud engineering and helping compliance professionals adopt to modern agile compliance principles. When he is not working, Max enjoys spending time with his wife Farah and three kids in Ohio.

Federal & Corporate agency cybersecurity experience

- USAF
- Army
- Navy
- DOS
- NRO
- NGA
- CIA
- NSA
- NASIC
- Dell
- IBM
- UFCU

Cyber & Technology Industry Credentials

- CISSP
- PMP
- Linux+
- Security+
- Network+
- ITIL-F
- Certified Scrum Master
- Digital Defensive Programming
- OWASP
- Threat Modeling

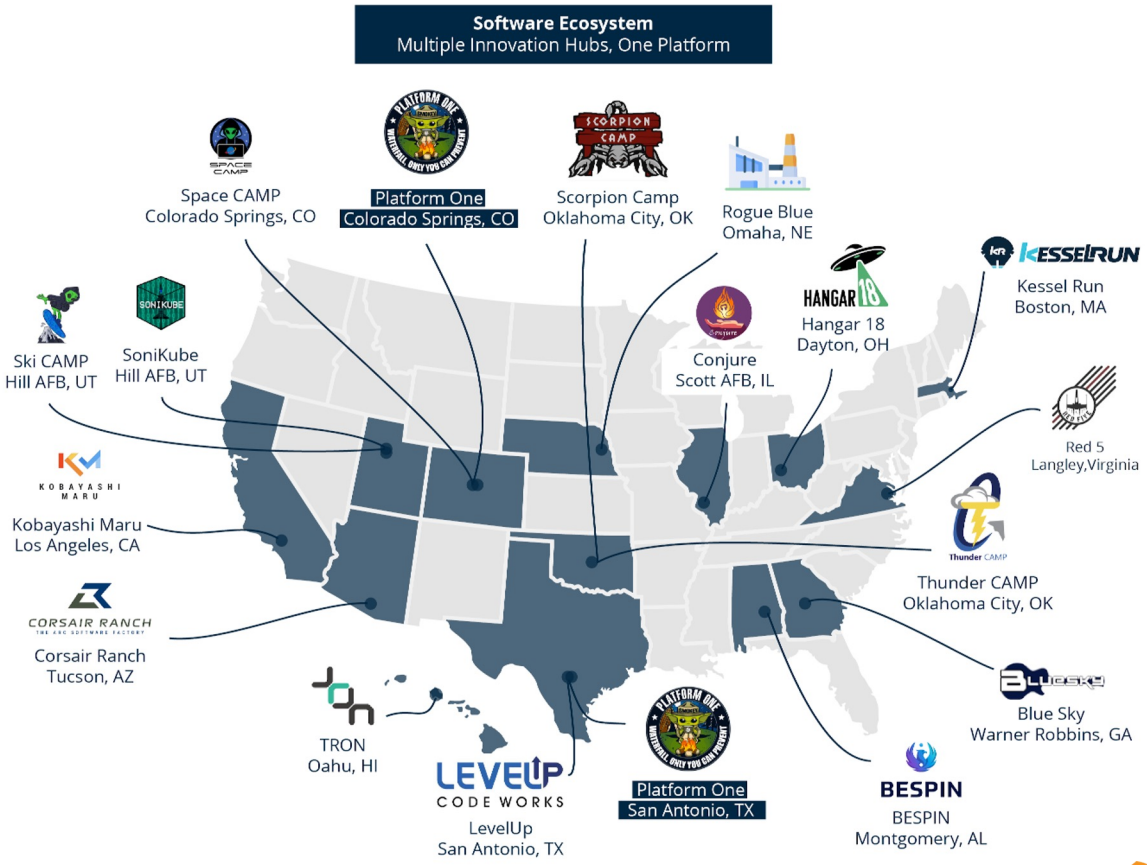
Agenda

- **The Modern Software Factory Challenges**
- **ATO in Context of DoD & Private Sector**
  - DoD RMF & FedRAMP
  - Commonalities in components
- **Component Aggregation**
  - What is it? Why do we need to do this?
- **Aggregation Techniques**
- **Basic Demonstration**
- **Future Initiatives**
- **Summary**
- **Q&A**

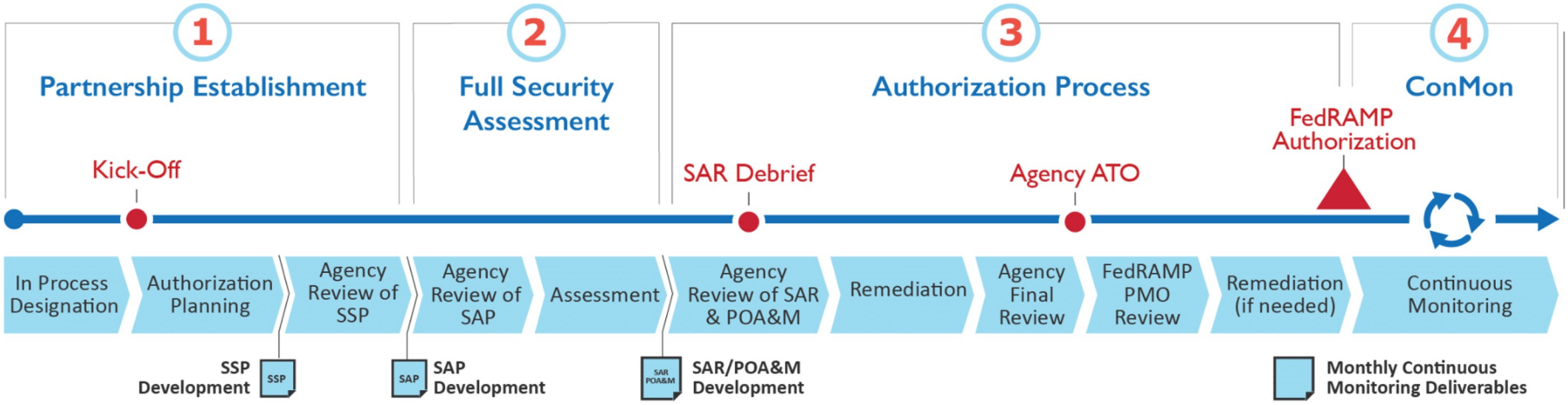
Software Factory Challenges

Software Factory Challenges

1. **Speed** - Slow approvals
2. **Scope** - What are we accrediting (process versus static packages)
3. **Methodology** - How are we accrediting? Continuous State



Understanding Current POVs | FedRAMP

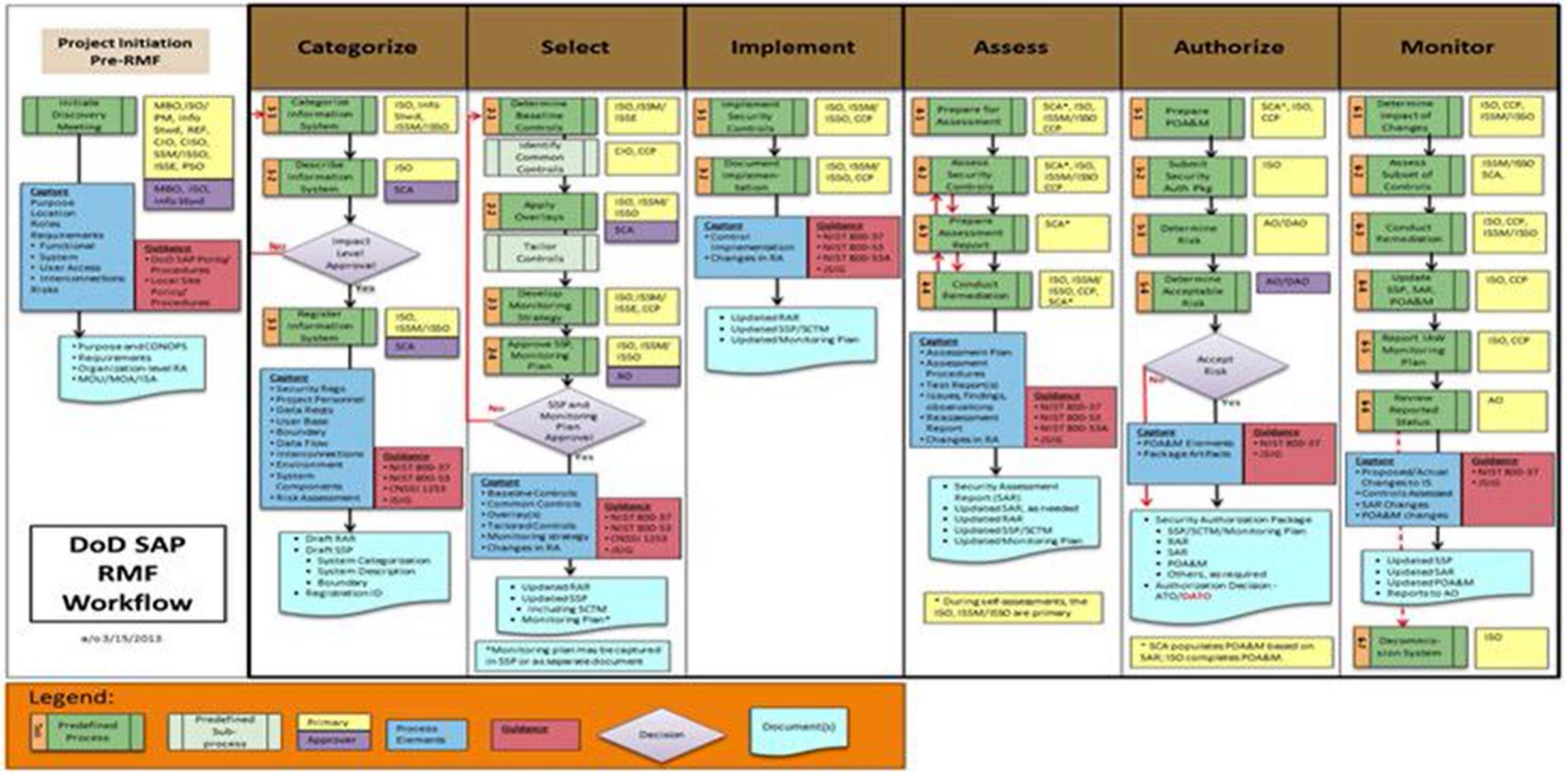


*SAP and SAR are developed by the 3PAO

FedRAMP

ATO in Context of DOD

Understanding Current POVs | DOD



Additional DoD Context

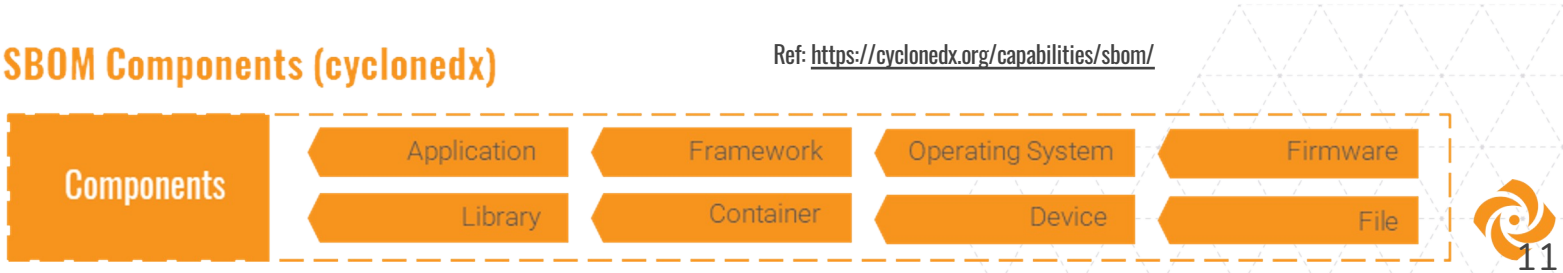
Language confusion - adding all OSCAL Components may not result in a "DoD Capability" for a "DoD Component"

- DoD Capability
  - DoDAF CV-2 (Capability Taxonomy)
  - May not be same as "OSCAL Capability"
- DoD Component
  - 2 CFR § 1125.937 - DoD Component.
  - Organizational level

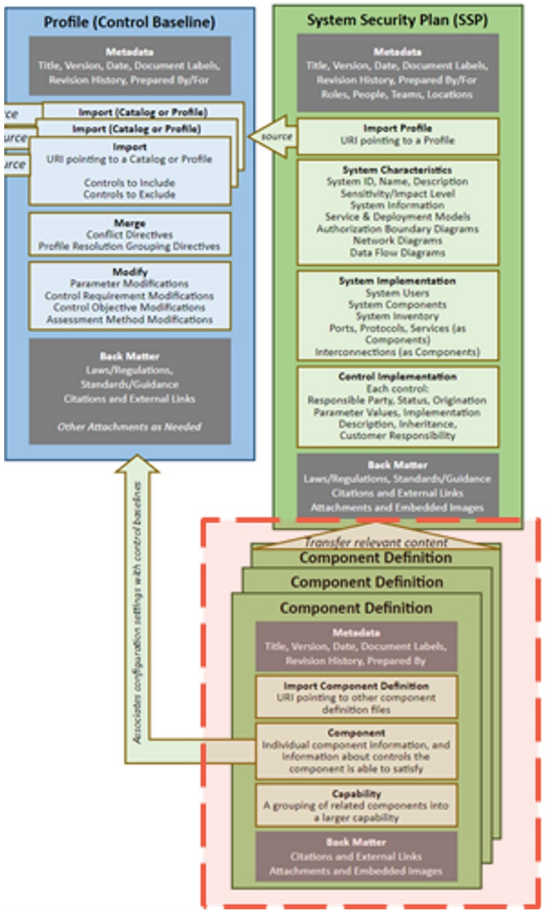
OSCAL Components, SBOM Components & DoD RMF

Reconciliation & Reconstruction

- SBOM Components
  - Lower level on the “component” hierarchy
  - Currently not part of traditional RMF (work in progress)
- Software Factory Technology Stack Components
  - PaaS, IaaS, and SaaS
  - Different components for each layer



OSCAL Component Definition



Purposefully Broad & Flexible

- Turn components into capabilities
- Encompasses vendors, organizations, hardware, Policies, Processes, software, etc.

The OSCAL component definition model represents a description of the controls that are supported in a given implementation of a **hardware, software, service, policy, process, procedure, or compliance artifact** (e.g., FIPS 140-2 validation). The component definition model is part of the OSCAL implementation layer.

The component definition model allows grouping related **components into capabilities**, and documenting how the combination of components in a capability together can satisfy specific controls that are not fully satisfied by a single component on its own.

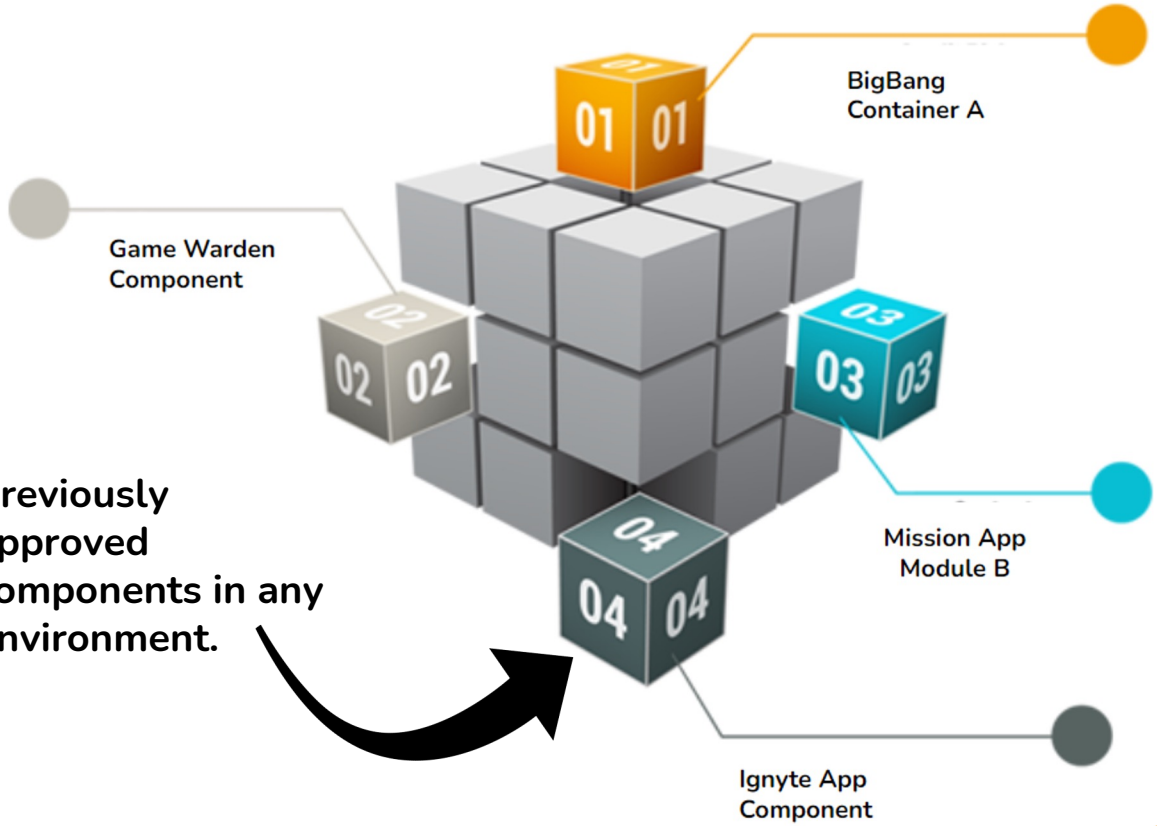
These component definitions can be used by organizations implementing the thing defined by a given component to provide a significant amount of implementation details needed when documenting a system's control implementation in a system security plan. This information can be used by the system security plan author as a starting point for their **work, saving time and cost.**

Aggregation Techniques

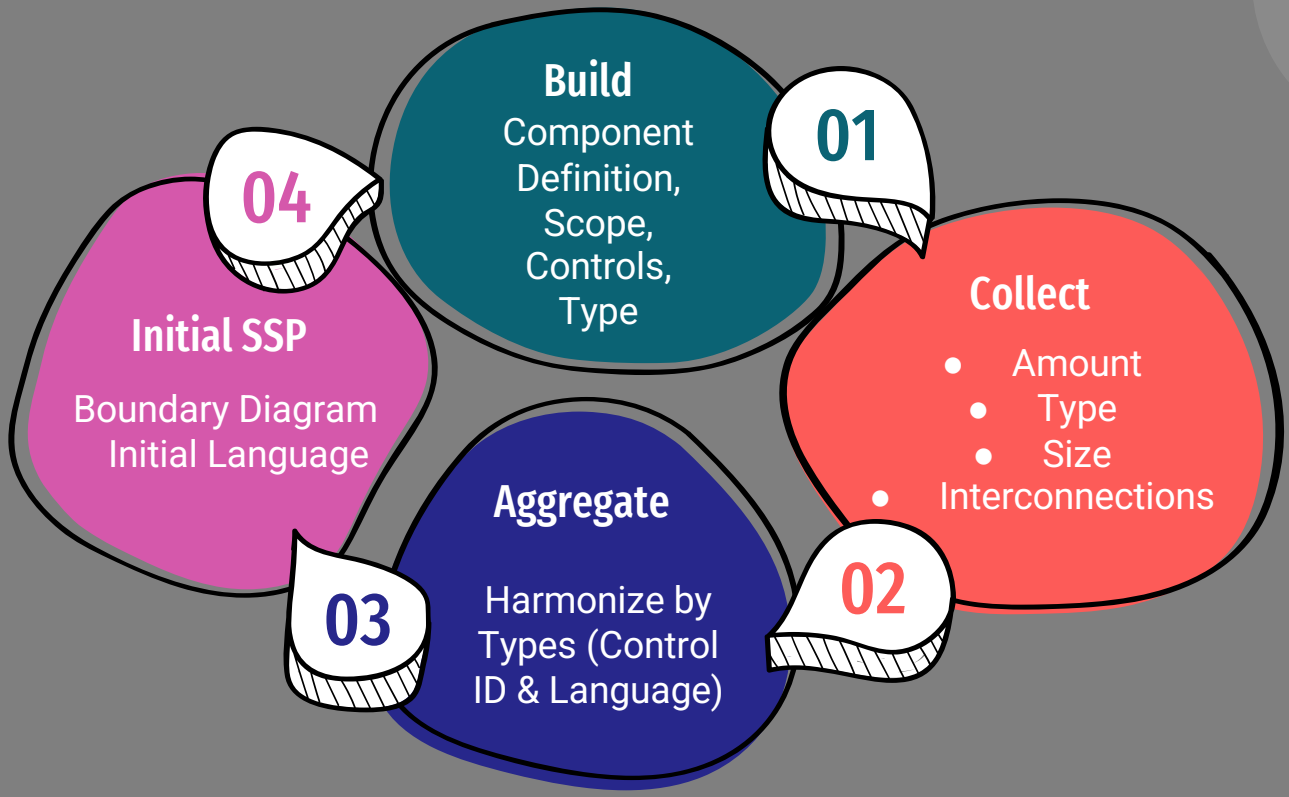
Why Aggregate?

Component Aggregation

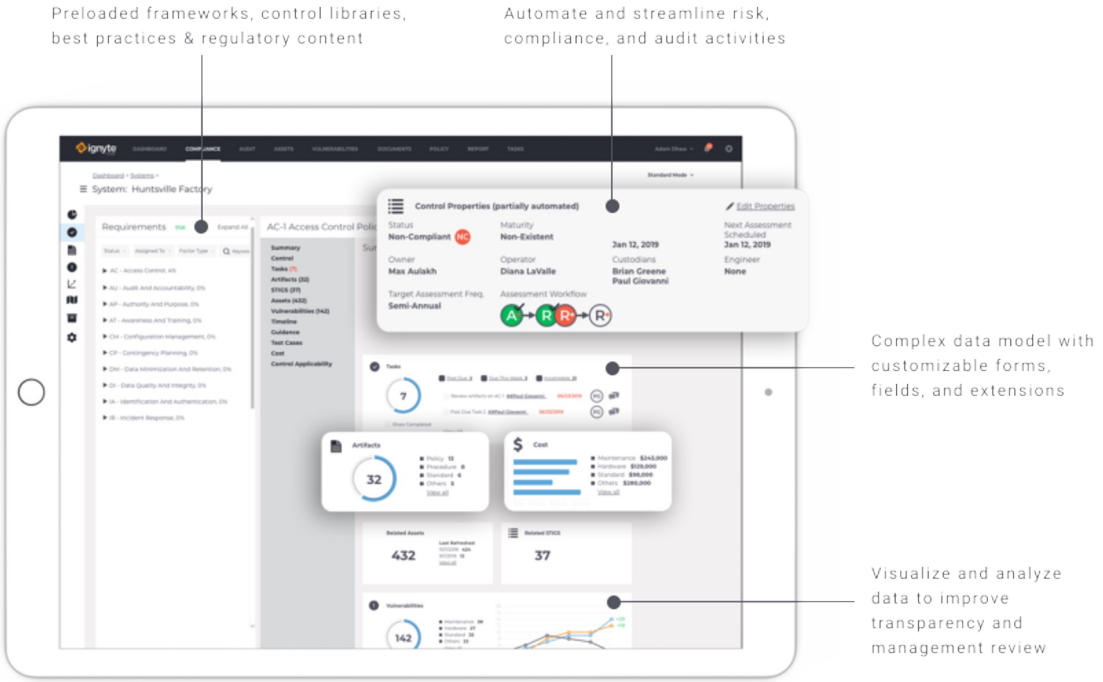
- Save time & money
- Faster initial SSP Delivery
  - Future potentials of a “Run-time based SSP”
- Reuse without knowing the target deployment environment

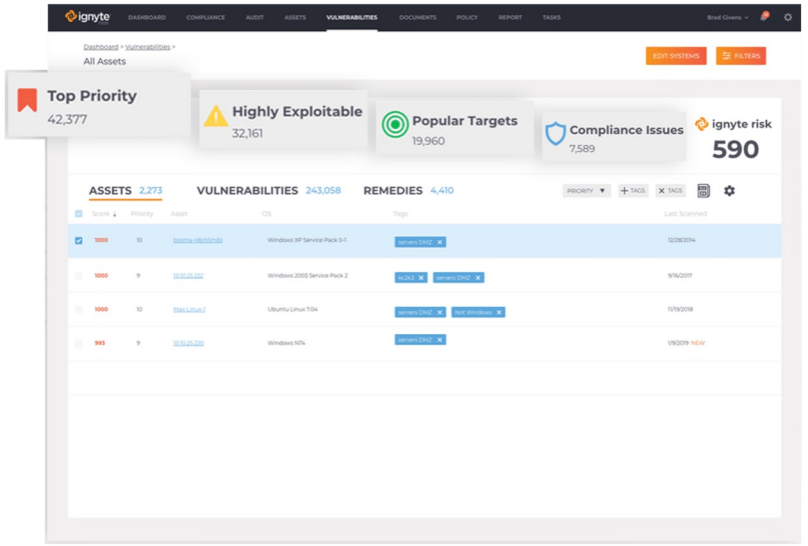


Our Initial Process



Component Aggregation Demo!





Manage ATOs (Moving Target)

Auto-build Components From SecOps Data - Source of Truth (Stream Data)

Future Initiatives

Ignyte OSCAL - Future

FedRAMP

Optimize FedRAMP Small Business Assurance Cases

Existing CRADA Software Factories Iron Bank Language Generation

Open Source (with permission) Component Collaboration SCF Integration

Let’s Summarize

1. Challenges | Reciprocity, Reuse, Speed, and Cost

2. The DoD Context | Language Confusion, SBOM, DoDAF, Reconciliation, and Reconstruction

3. Component aggregation process, future R&D, and Ignyte Demo

Contact Us:

www.ignyteplatform.com

info@ignyteplatform.com

max@ignyteplatform.com

susan@ignyteplatform.com

1.833.IGNYTE1

ignyte™ ASSURANCE PLATFORM