Modernizing Authorization Without Modernizing the System

Automated ATO for Legacy Platforms

DAFITC 2026 · August 24–26, Montgomery, AL



Speakers:

Shiv Bhuvanapalli,
Chief AI Officer, Inalab Group

Carlton Harris,
ISSO, Inalab Group

INALAB

THE PROBLEM

The System You Can't Modernize (Yet)

The documentation is frozen in time.

The system keeps evolving.

2023

INITIAL AUTHORIZATION

Evidence collected.
ATO approved.

2023–2026+

SYSTEM CONTINUES TO CHANGE

- New services deployed
- Configurations changed
- Users & accounts added or removed
- Patches applied (or not)
- Key personnel left

2026+

TODAY

SSP still describes the 2023 system.

DOCUMENTATION FROZEN IN TIME

Captures a snapshot of the past.

LIVE SYSTEM
CONTINUOUSLY EVOLVING

- New infrastructure
- New applications
- New dependencies
- New risks
- New configurations

REALITY

Evolving every day.
The gap grows wider every month.

Everyone knows the ATO is stale. Nobody wants to touch it.

Hundreds of legacy platforms across the federal enterprise operate under authorizations that no longer reflect their real security posture.

The gap between documentation and reality grows wider every month.

Stale authorization isn't just outdated paperwork—it's an unknown risk.
Adversaries don't check your ATO date before they attack.

THE PROBLEM

The Usual Advice — And Why It Doesn't Work

Modernize the System

Millions of dollars. 2–5 years. Scarce talent. Competing priorities.

The Reality

Most programs have **none** of these resources available simultaneously.

The Result

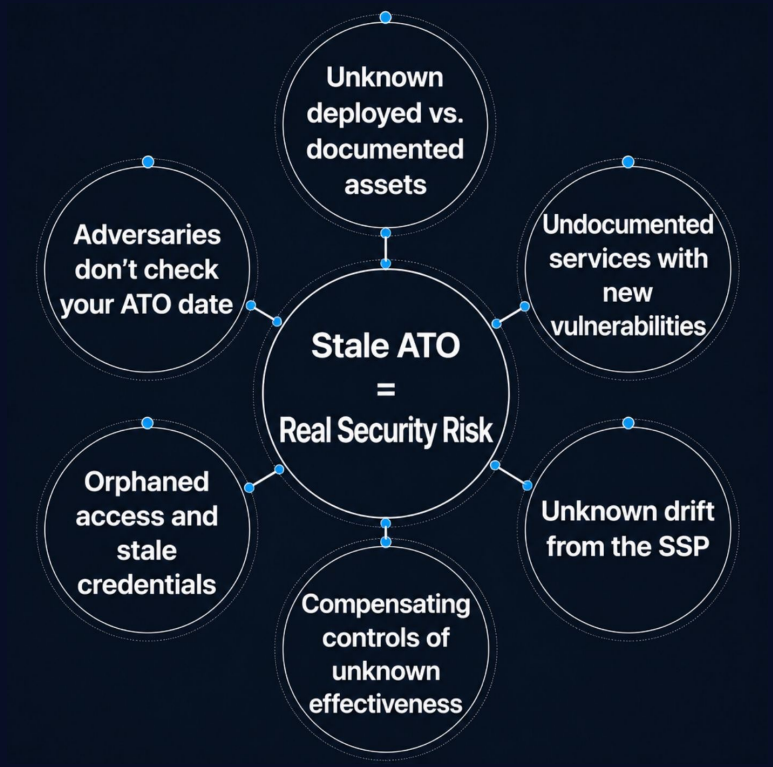
Stale ATO stays stale. Risk accumulates. The cycle repeats.

Meanwhile: mission risk continues to grow while documentation falls further behind reality. Every month you wait, the gap between your actual posture and your authorized posture widens.

You need authorization that reflects reality NOW – not in 2029.

THE PROBLEM

The Real Risk of Stale ATOs



A stale ATO is not a paperwork problem — it is a **genuine security liability.**

When documentation diverges from reality, defenders lose situational awareness across every dimension that matters.

> *Adversaries don't check your ATO date before they attack.*

THE SOLUTION

A Different Approach

Modernize the Authorization. Leave the System Alone.

AI Evidence Collection

Deploy AI-powered evidence collection alongside existing infrastructure – zero modifications required.

Connect to What Exists

Integrate with the infrastructure already running. No re-architecture, no new platforms.

Weeks, Not Years

Bring a paper ATO to continuous monitoring in 2–3 weeks. The system stays the same. The ATO becomes a living, continuously updated document.

THE METHOD

The Three-Phase Method

1 2 3

Phase 1

Evidence Discovery

3–5 Days

Deploy collectors, connect infra, pull evidence

Phase 2

Gap Analysis

5–10 Days

Compare evidence to SSP, AI narratives, ID drift

Phase 3

Continuous Monitoring

Ongoing

Scheduled re-collection, drift alerts, living auth

Three phases transform a frozen, paper ATO into a living authorization – measured in weeks, not years. Each phase builds on the last, creating a foundation for continuous compliance that requires zero modifications to the underlying legacy system.

THE METHOD

Why This Works for Legacy

1

No System Modifications

Zero changes to the legacy system. It runs exactly as it does today.

2

No New Infrastructure

Lightweight deployment into the existing environment. No re-architecture needed.

3

Connects to Whatever's Running

Cloud APIs, vulnerability scanners, config management, source repos, identity systems – if it runs, you can collect evidence from it.

The Core Principle

The evidence collection service deploys **alongside** existing infrastructure – never inside it.

It reads. It doesn't write. It observes. It doesn't touch.

Zero modifications to the legacy system. Period.

PHASE 1

Deploying Into the Existing Environment

A lightweight evidence collection service deploys into the existing VPC and connects to the data sources already present.

The data already exists. Nobody's been pulling it together.



The evidence collection service deploys alongside existing infrastructure — **never inside it.**

It reads. | It doesn't write. | It observes. | It doesn't touch.

PHASE 1

What You Discover

The discovery phase surfaces the current state of the system from every angle — **often revealing the first complete picture since initial authorization.**

Infrastructure Topology

Actual architecture vs. the 2023 diagram in the SSP. Often dramatically different.



Security Configuration

Current STIG/CIS scores — live, not from the last assessment cycle.



Vulnerability Posture

Real-time scan results correlated against documented compensating controls.

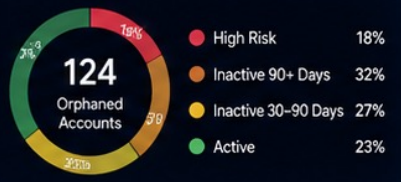
Open Vulnerabilities		
147	312	296
High	Medium	Low

COMPLETE SYSTEM DISCOVERY

All Evidence.
One Complete Picture.

Access State

Orphaned accounts, stale credentials, and privilege drift since initial authorization.



Change History

What's actually been modified since authorization — timestamped and traceable.

MAY 12	New S3 Bucket Created
JUN 03	Security Group Modified
JUN 21	EC2 Instance Deployed
JUL 08	IAM Policy Updated

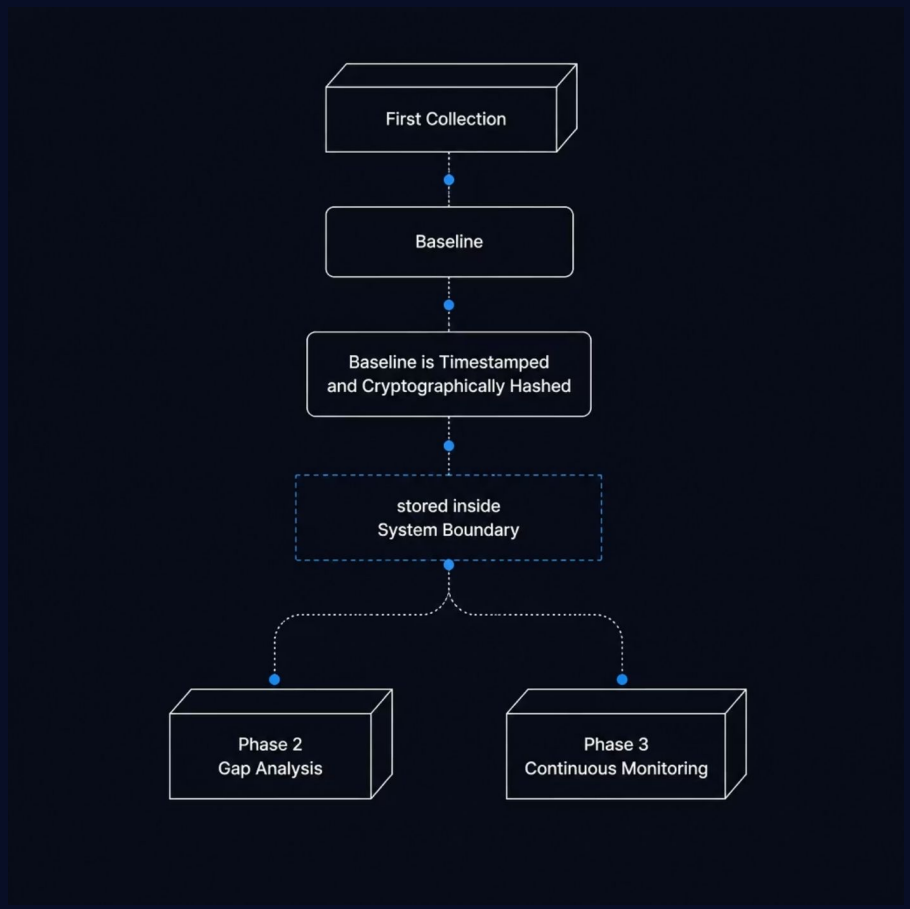
Often the first complete picture of the system **since initial authorization.**

- **Undocumented Services** — Routinely discovered
- **Configuration Drift** — Every layer
- **Access Gaps** — Across identities
- **Control Gaps** — Exposed

The discovery phase routinely surfaces services, configurations, and access that were **never documented.**

PHASE 1

The Evidence Baseline



A Foundation for Everything That Follows

The first evidence collection is more than a snapshot – it becomes the authoritative baseline against which all future system state is measured.

- Timestamped and cryptographically hashed for integrity
- Stored inside the system boundary – never leaves the authorization perimeter
- Feeds Phase 2 gap analysis immediately upon completion
- Seeds Phase 3 continuous monitoring cadence

Days – not months of manual evidence collection. The baseline that used to require a full assessment cycle now completes in 3–5 days.

PHASE 2

Identifying Drift with AI

AI compares collected evidence against the System Security Plan to identify **three possible outcomes** for every control, configuration, and system component.



MATCH

Evidence matches the SSP and is fully compliant.

- Control implemented as documented
- Configuration matches baseline
- No risk introduced

No action required
Continue monitoring

DRIFT DETECTED

Evidence differs from SSP but remains within acceptable risk tolerance.

- Configuration changed but still secure
- New service discovered with compensating controls
- Risk level acceptable with current controls

Document and Accept
Update records and continue monitoring

GAP FOUND

Evidence differs and introduces unacceptable risk.

- Control not implemented as documented
- New vulnerability without mitigation
- Access or configuration outside policy

Create POA&M Item
Mitigate, track, and validate closure

AI processes thousands of data points across every control, configuration, and component to determine the **true state of your system** — with unmatched speed and consistency.

- Thousands of Comparisons
- High Accuracy AI Analysis
- Minutes, Not Months
- Consistent Every Time

PHASE 2

AI-Powered Gap Analysis

AI compares what exists to what should exist and produces a complete gap analysis report with actionable insights.

INPUTS

Collected Evidence
Live data from all connected sources

System Security Plan
Policies, controls, and baselines

Control Catalogs
NIST 800-53 Rev. 5, DISA STIG, CIS, etc.

Environmental Context
Threat intel, asset criticality, business impact

AI ANALYSIS ENGINE

AI

Compares, correlates, and identifies gaps at scale

CONTROL MAPPING
Maps evidence to required controls

DIFFERENCE ANALYSIS
Identifies missing, partial, or extra implementations

RISK SCORING
Assesses risk based on impact and likelihood

SMART INSIGHTS
AI generates context-aware recommendations

REPORT GENERATION
Creates comprehensive, submission-ready report

GAP ANALYSIS REPORT

OVERALL COMPLIANCE

68%

Moderate Risk

CONTROL STATUS

Implemented	214
Partially Implemented	73
Not Implemented	28
Not Applicable	12

214	73	28	327
Implemented	Partial	Missing	Total Controls

TOP GAPS

- Unmanaged S3 bucket with public access
- Missing MFA for privileged accounts
- Outdated encryption protocol in use
- Missing audit logging on database

Prioritized Recommendations
Ranked by risk and effort

Minutes, Not Days
AI analyzes thousands of data points in minutes

High Accuracy
Consistent, repeatable analysis at scale

Context Aware
Understands relationships across controls and assets

Actionable Output
Clear gaps with prioritized, practical recommendations

PHASE 2

AI-Powered Narrative Generation

AI transforms gap analysis findings into clear, consistent, **assessor-ready narratives** mapped to **NIST SP 800-53 Rev. 5.**

1. INPUTS

- Gap Analysis Findings
- Control Requirements (NIST SP 800-53 Rev. 5)
- Existing SSP & Policy Content
- Environment & Business Context

2. AI ANALYSIS



AI correlates evidence, control requirements, and context to understand what the system actually does vs. what it should do.

3. NARRATIVE GENERATION



AI generates clear, consistent narratives with rationale, evidence citations, and compensating control explanations.

4. HUMAN REVIEW



Security professionals review, validate, and refine AI-generated content before finalizing.

OUTPUTS

Control-by-Control Security Narratives
Clear, structured, and assessor-ready

Evidence References
Direct links to collected evidence and data sources

Compensating Control Rationales
Justified, documented, and risk-informed

SSP Updates
Ready-to-integrate content for the latest system state

From findings to fully-formed narratives — **in hours, not weeks.**

DRASTICALLY FASTER
Generate hundreds of narratives in a fraction of the time.

CONSISTENT & ACCURATE
Eliminate inconsistencies. Ensure alignment with NIST SP 800-53 Rev. 5.

RISK-INFORMED
Built-in rationale and evidence mapping enhances defensibility.

HIGHER QUALITY
Clear, professional narratives that pass assessor scrutiny.

PHASE 3

Weeks, Not Years

AI-powered automation compresses the authorization timeline from years of manual effort to weeks of intelligent execution.

TRADITIONAL ATO APPROACH

12 – 18 Months

Evidence Collection Manual collection from disparate sources	2 – 4 Months
Documentation & Analysis Manual analysis, correlation, and documentation	3 – 6 Months
Narrative Writing Manual security control narratives and rationale	2 – 4 Months
Package Assembly & Review Compile, review, revise, and validate	2 – 3 Months
Assessment & Authorization Assessor review and authorization decision	2 – 3 Months

TOTAL TIMELINE: 12 – 18 MONTHS

VS.

AI-POWERED ATO APPROACH

2 – 3 Weeks

AI Evidence Collection Automated collection from all connected sources	2 – 3 Days
AI Gap Analysis AI-powered analysis and drift identification	2 – 3 Days
AI Narrative Generation AI drafts control narratives and rationale	2 – 3 Days
Auto-Package & Validation Automated assembly and quality validation	3 – 4 Days
Assessment & Authorization Accelerated assessor review and decision	5 – 7 Days

TOTAL TIMELINE: 2 – 3 WEEKS

From years of manual effort to weeks of intelligent execution.

Up to 25x Faster Authorization

Always Current. Never Stale.

Lower Cost Less Manual Effort

Reduce Risk Continuous Visibility

PHASE 3

Keep It Current

- Once package reflects reality, keep it there
- Scheduled re-collection:
  - Stable systems: weekly
  - Active systems: daily
- Drift detection: Compare against baseline, alert on security-relevant changes
- Automated updates to SSP as evidence changes

> *Never let the package go stale again.*

PHASE 3

What Drift Detection Catches

Configuration changes: Security settings modified

Access changes: New accounts, privilege escalations, orphaned access

Vulnerability changes: New CVEs, patches applied/missed

Infrastructure changes: New services, decommissioned systems

Compliance changes: STIG/CIS score changes

Each event triggers: what changed, when, security impact, recommended action.

> *Reality changes. Now your documentation keeps up.*

Smart Prioritization

Drift detection ranks what demands attention first, reducing noise and alert fatigue.

🔴 Critical — Immediate

- MFA disabled on any account
- New admin/privileged access granted
- Unexpected port exposure detected

🟠 High — 24 Hours

- STIG score drop >5%
- New unpatched CVE introduced
- Firewall rule modification

🔵 Medium — Weekly Review

- Configuration parameter changes
- New services deployed
- Software version updates

THE RESULT

An ATO That Never Goes Stale

From a decaying, paper-based authorization to a living, continuously-validated state of security.

BEFORE: THE DECAYING ATO

A Snapshot in Time That Ages Poorly



OUTDATED
Evidence collected once, years ago.

DRIFTING
The environment changed. The ATO didn't.

BLIND SPOTS
Unknown risks in undocumented changes and services.

RISK ACCUMULATES
Increased exposure. No visibility.

MANUAL & SLOW
Re-authorization takes months or years.

AI-POWERED AUTOMATION

WEEKS, NOT YEARS

AFTER: THE LIVING ATO

Always Current. Always Defensible.



ALWAYS CURRENT
Live data. Real-time visibility. Always up to date.

COMPLETE VISIBILITY
Know what's running, what changed, and why.

RISK REDUCED
Gaps identified early. Issues addressed fast.

CONTINUOUS ASSURANCE
Evidence collected on a schedule. No scramble.

ASSESSOR READY
Accurate, complete, and defensible at any time.

THE OUTCOME

Reduced Risk
Close gaps before they become incidents.

Faster Decisions
Real-time insights for faster action.

Lower Costs
Eliminate rework. Reduce manual effort.

Increased Confidence
Defensible authorization at all times.

Better Outcomes
Secure the mission. Support the warfighter.

Sustainable Process
A repeatable model for continuous authorization.

THE CHALLENGE

The Security Valley

- The problem: System works but can't get authorized
- The gap: 6–18 months stuck in limbo
- The cost: Mission capability gap while waiting for paperwork
- The outcome: Modernization projects go to die

New capability built. Can't deploy. Can't authorize. Can't operate.

> *Where modernization projects go to die.*

THE SOLUTION

Shift Security Left Into Development

- **Embed compliance scanning into development pipeline**
- **STIG validation on every build**
- **IL5 checking on configurations**
- **Vulnerability scanning at commit**
- **Evidence collection from Day 1**
- **Result: By deploy time, package is mostly done**

Authorization is an update, not a cold start.

THE SOLUTION

Bridging Legacy to Modern

- **While legacy runs:** AI keeps its ATO current
- **While new system builds:** Compliance scanning from day 1
- **At cutover:** Neither has a gap
- **Result:** No security valley, no authorization delay

Legacy stays authorized. New system arrives pre-authorized. Transition is seamless.

> *No gap in authorization. No security valley.*

REALITY CHECK

Honest Limitations

- **Minimal cloud footprint:** More custom work to collect evidence
- **Air-gapped systems:** Deploy self-hosted AI, not cloud-based
- **No scanners:** Deploy scanning infrastructure first
- **eMASS integration:** Human-in-the-loop for final submission
- **Organizational resistance:** Start with one system, show results, scale

Honest about where this is harder. Still doable.

THE OPPORTUNITY

The Scale of the Problem

- DAF operates thousands of systems
- Unknown percentage have stale ATOs
- Can't rebuild all of them
- Don't have 12–18 months per system
- But: CAN deploy evidence collection in weeks
- Impact: Fix authorization without fixing the system

> *Thousands of stale ATOs. Fixable without rebuilding a single system.*

SUMMARY

Key Takeaways

1. Don't need to modernize the system to modernize authorization
2. Evidence collection deploys alongside existing infrastructure—no modifications
3. Gap analysis in days, not months
4. Continuous monitoring keeps authorization alive
5. For active modernization: embed compliance from day 1
6. Start with one system. Show results. Scale.

> *Pick your worst stale ATO. Start there.*

Questions?

Shiv Bhuvanapalli, Chief AI Officer, Inalab Group
sbhuvanapalli@inalabgroup.com

DAFITC 2026 · August 24–26, Montgomery, AL







