

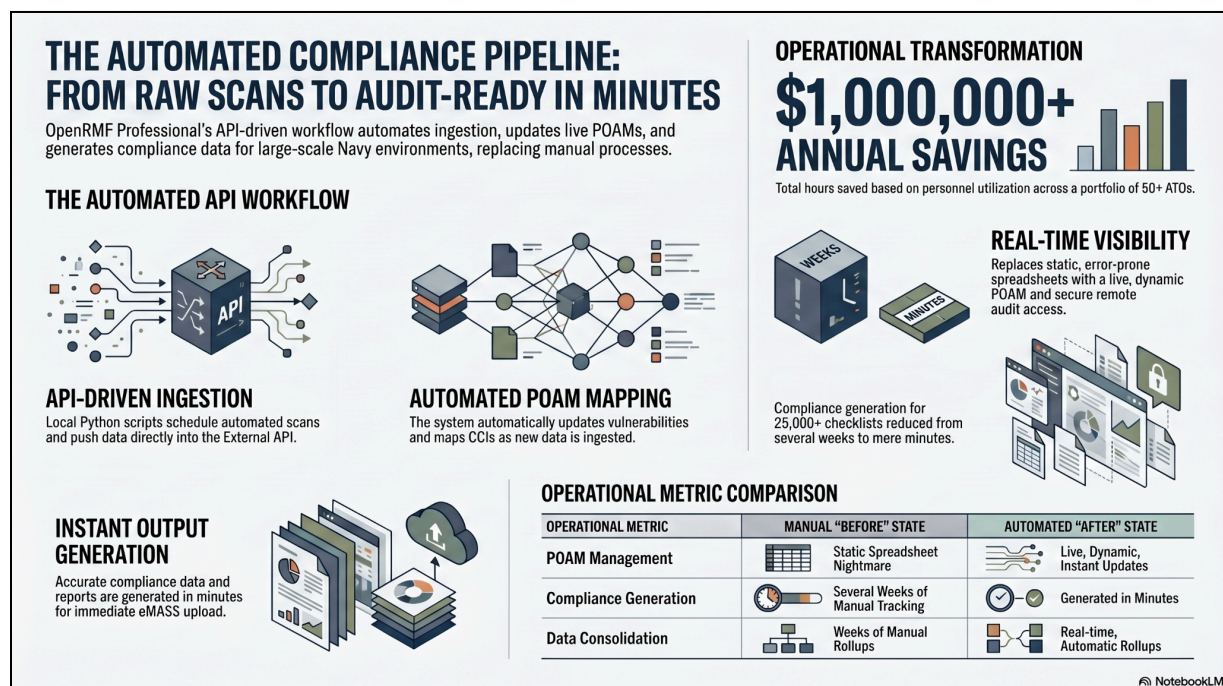
# Case Study: Enterprise Scale Transformation for a Large Navy Customer

## Executive Summary

Managing enterprise-level accreditations across unclassified and classified networks presents a massive scalability challenge. For one of our large Navy customers, managing over 50 Authority to Operate (ATO) packages—including a massive 4,000-device ATO encompassing over 25,000 individual checklist files—reached a manual breaking point.

They had separate teams emailing in checklists, patch vulnerability PDFs, and POA&Ms to team leads and the leads worked to integrate all that data into one POA&M and one structure manually. Tracking open vulnerabilities, answering data calls, and verifying truthful data took days per team. And generating compliance across all data took weeks to complete.

Implementing **OpenRMF Professional** transformed their cybersecurity posturing from a reactive, manual nightmare into an automated, continuous compliance powerhouse.



## The Operational Divide: Before vs. After OpenRMF Professional

| Operational Metric                           | The Manual "Before" State                                                                                                          | The Automated "After" State                                                                                                          |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Data Consolidation &amp; Rollups</b>      | Fragmented teams emailed siloed POAMs and uploaded raw files to SharePoint, requiring weeks of manual consolidation.               | <b>Team Subpackages</b> allow localized data management with automatic, real-time rollups to the top-level ATO.                      |
| <b>POAM Management</b>                       | A static, error-prone spreadsheet nightmare to keep updated and truthful for eMASS uploads.                                        | A <b>live, dynamic POAM</b> that tracks and updates vulnerabilities instantly as data changes.                                       |
| <b>Compliance Generation</b>                 | Calculating compliance across all controls and CCIs took multiple personnel <b>several weeks</b> of manual tracking.               | Full compliance mapping is generated <b>in minutes</b> across all data, with absolute truth and accuracy.                            |
| <b>Data Integrity &amp; Validation</b>       | Tracking checklist types took days. Validating if "Not a Finding" or "N/A" statuses were properly justified was nearly impossible. | Automated scanning easily identifies data gaps where justification details are missing, preventing teams from "cheating the system." |
| <b>Automation &amp; Pipeline Integration</b> | Entirely dependent on manual data calls, slow email response times, and physical file transfers.                                   | Fully integrated <b>External API</b> with local Python scripts to schedule scans, ingest data, and auto-generate reports/emails.     |
| <b>Assessment &amp; Audit Readiness</b>      | Assessors required massive emailed ZIP files or local file system access, slowing down review timelines.                           | Assessors utilize <b>secure web access</b> to remotely view past/present history and track scheduled fix completion dates.           |

## Deep Dive: The Reality of Manual Compliance vs. Automated Efficiency

**The Manual Burden:** Understaffed teams were buried under large infrastructure and layered accreditations with complex inheritance structures. Device drift went unnoticed, data calls required chasing teams via email, and the sheer volume of data (25,000+ checklists for a single ATO) resulted in compromised accuracy and delayed ATO submissions.

With OpenRMF Professional, the Navy customer unlocked unprecedented visibility and efficiency:

- **Host-Level Granularity:** Easily track patch vulnerabilities, compliance drift, and anomalies across thousands of devices simultaneously.
- **Dynamic Inheritance:** Inheritance pathways are mapped effortlessly. When an inherited package updates, downstream teams are automatically notified of the change.
- **Truthful Data Calls:** Cross-team data requests that used to take days are now answered instantly with comprehensive, system-wide reports.

## The Bottom Line: ROI and Impact

The transition from a manual, document-heavy process to OpenRMF Professional's automated framework didn't just improve cyber hygiene—it delivered a massive return on investment.

- **Data Accuracy:** Compliance data is now accurate, auditable, and instantly ready for eMASS upload.
- **Resource Optimization:** Shifting from weeks to minutes for compliance generation freed up critical personnel to focus on actual system defense rather than administrative paperwork.
- **Financial Savings:** Across their portfolio of 50+ ATOs, the total hours saved based on personnel utilization calculated out to **over \$1,000,000 saved annually**.

## Take Control of Your RMF Pipeline

Don't let manual paperwork dictate your command's cyber readiness posture. Eliminate compliance bottlenecks, achieve 100% asset visibility, and slash your ATO turnaround times with automated workflows.

## Schedule a Live Demo or Start Your Evaluation Today

Ready to see how OpenRMF Professional can transform your RMF process? Visit **Soteria Software** online to take the next step:

- **Request a Live Demo:** See a tailored walkthrough of the automated API pipeline, live POA&M engine, and executive dashboards.
- **Fully Evaluate the Platform:** Download and test the software directly in your own environment to experience the time savings firsthand.

**Get started now at:** [www.soteriasoft.com](https://www.soteriasoft.com)