SOTERIA SOFTWARE

OpenRMF® Professional:

Cyber Compliance Automation That Works

Executive Summary

Performing cyber compliance for your systems, networks, and accreditation boundaries can be exhausting if you are still doing all the work required manually. Scanning your machines and devices, tracking checklists and spreadsheets for updates, keeping track of your plan of action and milestones (POA&M), and trying to keep them up-to-date manually is not sustainable if you are doing even just part of that manually.

The amount of data to collect, track, analyze, and report is more and more overwhelming. Which means automation ***must*** come into play to allow confidence and trust to permeate the process. And de-stress the directors, managers, staff, assessors, and government officials at the same time.

The founders of Soteria Software have been working with cyber compliance since 2004. And they noticed over and over again that organizations, whether small or large, were still doing things manually like they did way back in 2004 when they met at a NAVSEA base in Indian Head, Maryland. Even to this day! So they put their skills, knowledge and experience into action to innovate around automating cyber compliance. And created their flagship solution: OpenRMF® Professional.

OpenRMF® Professional is a purpose-built cyber compliance automation and collaboration platform from **Soteria Software.** It is designed to radically reduce the time, cost, errors, and manual effort associated with achieving and maintaining your cyber compliance, accreditation, and continuous monitoring. And perform that automation wherever you need it: on premise, in the cloud, in a hybrid setup, or even on an air gapped network.

It works across various cyber frameworks like RMF, FedRAMP, CMMC, ISO, and more. And consolidates data, automates analysis, and provides teams with a single authoritative source-of-truth for compliance status and trending information — all within a web-based, integratable, and team-centric environment.

The result is a solution that automates 90+% of the normal tasks associated with tracking your cyber compliance. It gives you results from the scans you are already doing. It tracks gaps in compliance for you to fix. And it does this in a collaborative way across your team so everyone can do their part toward automating your cyber compliance with truthful, consistent data across any of your accreditation boundaries.

Manual Compliance is Not Sustainable

Organizations subject to Risk Management Framework (RMF), FedRAMP, CMMC, or other compliance requirements face a set of common, entrenched challenges to track their compliance. This is made worse by doing any or all of these manually. There are several key issues that stand out when you do not automate your compliance.

Fragmented Data and Manual Processes

Compliance workflows typically depend on *disparate files* (SCAP/ACAS scans, STIG checklists, patch reports, software scans) that are manually edited, shared, and tracked — often in spreadsheets, PDF files or siloed tools that are not linked and correlated to each other and to the larger compliance controls required for accreditation. And these all are only a snapshot in time.

Teams end up spending hours reconciling checklist results, updating POA&M tables, tracking detailed compliance across disparate data, and generating documentation manually rather than focusing on real security improvements.

Lack of a Single Source of Truth

Without centralized, unified data across all types of scans and results, your status reporting and compliance traceability become error-prone and time-consuming. This increases the risk of inaccurate reporting to management, authorizing officials and your assessors.

For example, your network team does patch vulnerability scans on machines and devices for operating system patches. Those are exported in CSV or PDF and emailed to the program analyst tracking the POAM and generating vulnerability numbers for monthly reports. They also perform SCAP scans or Audit Compliance scans and generate at least one file for compliance scan results per machine or device. Those are also emailed to the same person for the same reasons. Then your developers and database administrators are filling out checklists to track compliance with databases, software development, web applications and other applications.

All these individual files have to be kept up to date, versioned, tracked for changes, and secured. And the SCAP scan results must be updated quarterly for any updated checklists or benchmarks run to track compliance of those same machines. You also

need to use all results across all devices for accurate reporting, and must have any updates emailed to the same person or put into the same shared folder for use and tracking compliance going forward.

Finally, your information system officer or engineer must use all data from scans, documents, and statements to track compliance against the chosen framework (e.g. Risk Management Framework) according to the version, levels, overlays (extra controls) as well as any tailoring in or out of specific controls based on the requirements. And each individual checklist has one or more vulnerabilities with one or more references through a control correlation identifier that maps to the controls for the chosen framework and levels.

And each time there is a change, it may require an update of the real compliance and risk. This compliance tracking is tedious, time consuming and prone to mistakes and missing issues when done manually. At the same time it is extremely important to gauge your compliance with the risk framework as well as to track with open vulnerabilities and mitigations to true risk for this accreditation package to be accurate.

This critical component and culmination of your compliance work, your continuous monitoring of compliance, is also undermined when scan results, vulnerabilities, and compliance documents exist in separate tools and locations. Not only do you need to manually track them, manually correlate them to every control and control correlation identifier (CCI), and track the overall status of data to know where you and your team stands as far as compliance gaps and mitigations. You must keep up with changes across all devices, policies, procedures, and risk mitigations.

Team Collaboration and Workflow Bottlenecks

There are also differing tools and file formats that impede teamwork. Only a fraction of your staff can meaningfully interact with all related compliance data in real time when it is spread across hundreds of files and file types. This is the case whether it is because of limited access to the tools, the scan results, or understanding the results as it pertains to the cyber compliance framework.

Your team collaborating over disconnected files slows the process, silos information, and makes tracking compliance as well as achieving accreditation months longer than it actually needs to be.

On top of that, the manual editing of evidence, checklists, and POA&M statuses slows response cycles and frustrates stakeholders. And the data is out-of-date if any of the items mentioned in the POA&M changes as it is generated statically at a moment in time. Additionally, any history of changes, tracking of vulnerability history burndown, and tracking of POA&M changes is nowhere to be found when performed across separate files.

Even running client based tools, after performing the collection of all required data files manually, to get a static analysis-in-time is still time consuming and error prone. And it is out of date ***immediately*** once any of the data changes. Not only do you need to have that client tool installed/configured on every single machine that needs it. You also need to download and copy all current data over to it for it to be used each time manually. And once done the results must be sent out to every person required to or just interested in seeing the results.

High Operational and Resource Costs

A large issue when you and your team are performing manual compliance procedures, is that it drains staff time, induces burnout, and inflates operational costs — sometimes materially impacting the ability to even meet accreditation deadlines. And this doesn't include the loss of inherent knowledge with staff turnover.

As mentioned earlier, the traditional solutions are either file-centric, closed proprietary offerings, or require significant customization to support role-based team workflows. You have a number of files and formats mentioned earlier:

- SCAP scan / Audit Compliance results that must be turned into checklists
- Patch Vulnerability results, normally tracked in spreadsheets or PDFs
- Compliance Statements for policy and procedure tracked in spreadsheets
- The list of controls and CCIs to meet, tracked in spreadsheets
- POA&M, tracked in spreadsheets
- Individual compliance by source results tracked in spreadsheets, if at all
- Additional files such as SSP, SAR, RAR tracked in spreadsheets

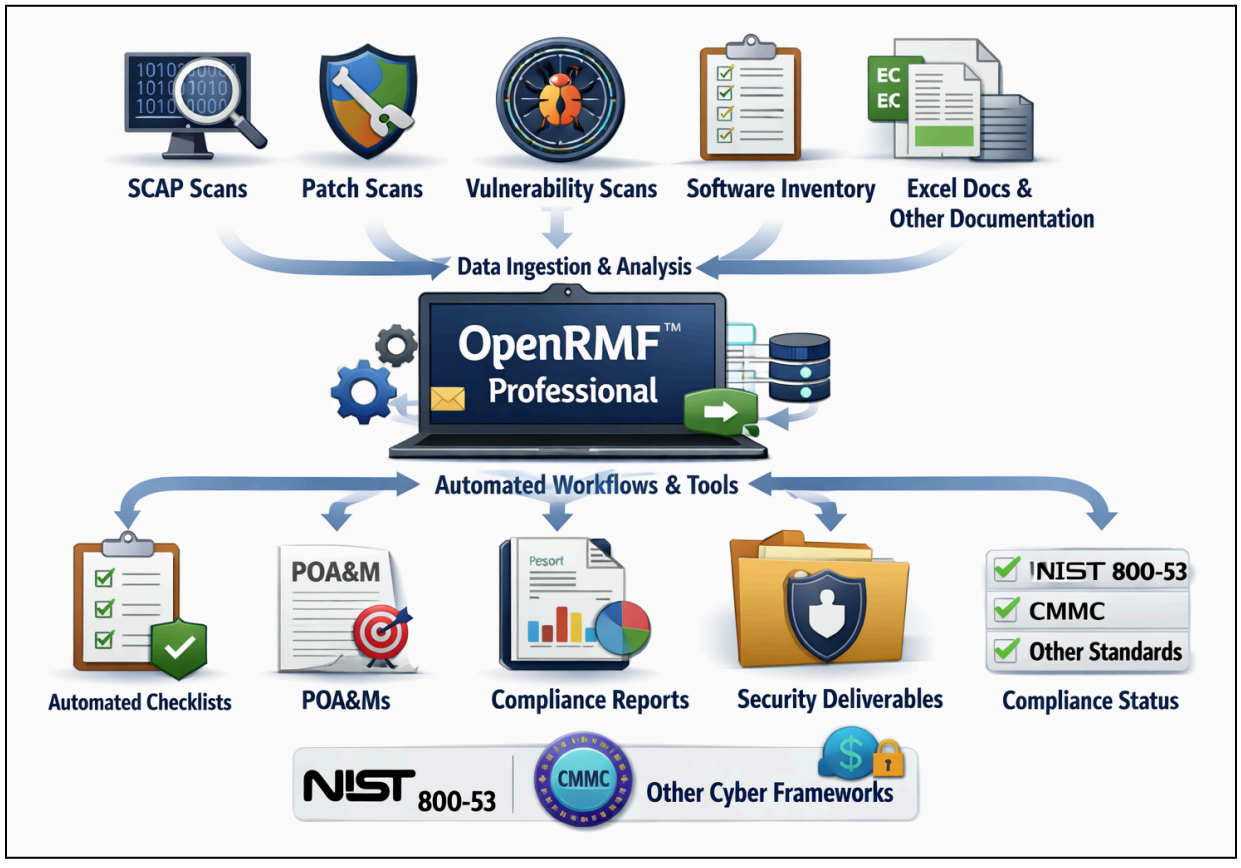
Does it sound like a lot of work to track manually? That is because it is. And cognitive overload and burnout of personnel adds to the stress of doing this job and doing it right. In short, **manual compliance is a systemic risk and drag on mission readiness** for organizations needing secure, accurate, and repeatable compliance operations.

The Solution: OpenRMF® Professional

The solution is to automate as much of this process as possible. And do that with a centralized solution specifically designed to alleviate these problems and bottlenecks. That is built to integrate with other existing processes and solutions where applicable, not yet another silo of information.

That is why we built OpenRMF® Professional – a **web-based compliance automation platform** that ingests, correlates, and tracks compliance data across frameworks, scan sources, vulnerabilities, and system packages through a unified interface. It is designed to take in your scan results and build your accreditation packages from the ground up.

OpenRMF® Professional is your Single Source of Truth for your compliance data for the whole team to use and collaborate around. It is a centralized repository for all compliance artifacts — checklists, SCAP/ACAS/Nessus patch and audit results, POA&M, hardware/software inventories, POA&M, reportings and more.



Automated Scan Ingestion and Tracking

Our solution has automated ingestion and processing for your various compliance scan results that you are already doing in your daily job right now. You can upload compliance scan results (e.g., Nessus, Rapid7, SCAP), and OpenRMF® Professional normalizes and links the data against controls and CCIs automatically using STIG Checklists. And you can easily export out the checklists in various formats such as CKL, CKLB or even MS Excel to external personnel or for use in your program of record.

You also can upload patch vulnerability scan results (e.g. Nessus) to track not only patch vulnerabilities. It also automatically tracks software, hardware devices (linked to checklists as well), as well as ports, protocols, and services from those existing scans. And it tracks data and vulnerability burn down numbers automatically as well, at the top accreditation level as well as each device and checklist.

Live POA&M

One of the unique features of OpenRMF® Professional is the Live POA&M. The POA&M tracks all open and not yet reviewed items across patch vulnerabilities, checklists, compliance statements, inherited controls and more. That allows a continually updated Plan of Actions and Milestones (POA&M) with bi-directional traceability and powerful bulk edit capabilities to rapidly correct or annotate items.

Export out to your proper program of record format such as eMASS or MCCAST, or even a general format to report to your organizations as required.

Simple Pricing and Installation

Our OpenRMF® Professional solution is installed by any of your normal network and system administrator support staff. It does not require paying one of our consultants $200/hour over a few week period just to customize the application to get it ready for use. It is purpose built to perform automated compliance well from Day 1 using your own data.

We also price by only two things – the number of installations and the number of active accreditations you need to track per installation. That is it. Unlimited users, CPU, memory, drive space, devices, and everything else. So you know exactly what the cost is up front, and can figure it out without a Master’s Degree in Microsoft Excel.

Team Collaboration and Role-Based Access

Your accreditation packages in OpenRMF® Professional support multi-tenancy and role-based access so teams can work concurrently without data leakage or confusion. Every member of your team can access only the data they need with the permissions required in a (RBAC) least-privileged manner.

You also can use our unique Team Subpackage feature to separate out a larger accreditation package and give your team access to only the data they need to view and manage. All the while your information security officials still track all data, changes, and trends at the top level accreditation package. You have need to know and separation of duties accomplished using the Team Subpackage feature.

APIs and Integrations

OpenRMF® Professional ***does not create yet another silo of information***. It includes an external API that allows you to interact with the automation and features programmatically. This allows uploading of scan data to track and automatically create/update checklists and compliance. It also allows downloading of scan results and data, generating your compliance and more all from calling APIs with proper permissions and roles. And it enables integration with DevSecOps pipelines, automated scan ingestion, and external BI/reporting systems as well.

Along with the external API, our solution integrates with task management software such as Atlassian Jira and ServiceNOW to track items and issues. It connects to Nessus scanners to automatically ingest scan data. And it connects to software scanners to ingest software vulnerabilities across your accreditations as well.

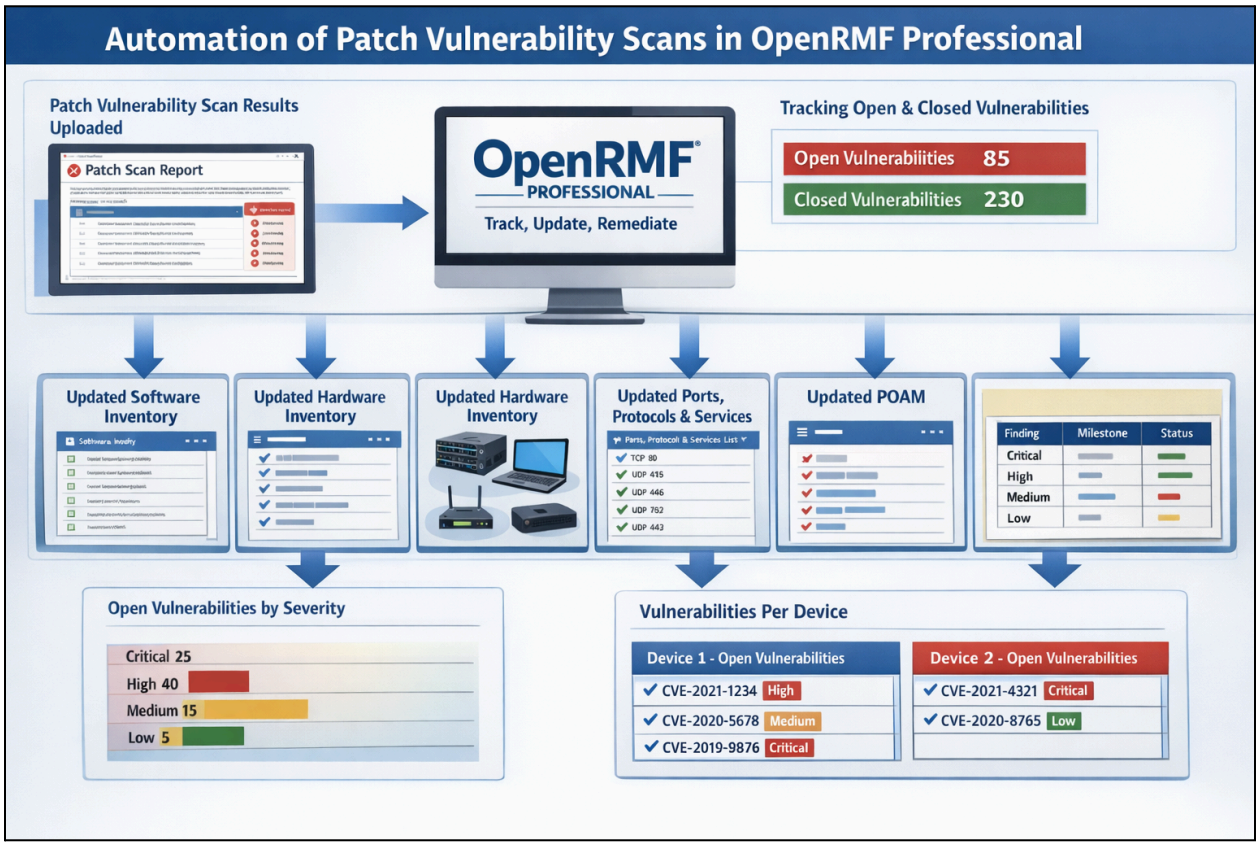
OpenRMF® Professional plays a key role in your overall cyber security mesh architecture to solve your compliance needs, while integrating with the rest of your team and your other cyber software investments.

Hyper Automation

OpenRMF® Professional also includes things you never thought possible because currently your team's data is stored in separate files. And your team is maxed out on time doing manual processes across all those separate files.

When automating cyber compliance takes over, you can perform the following functions (and more) easily using our purpose-built solution:

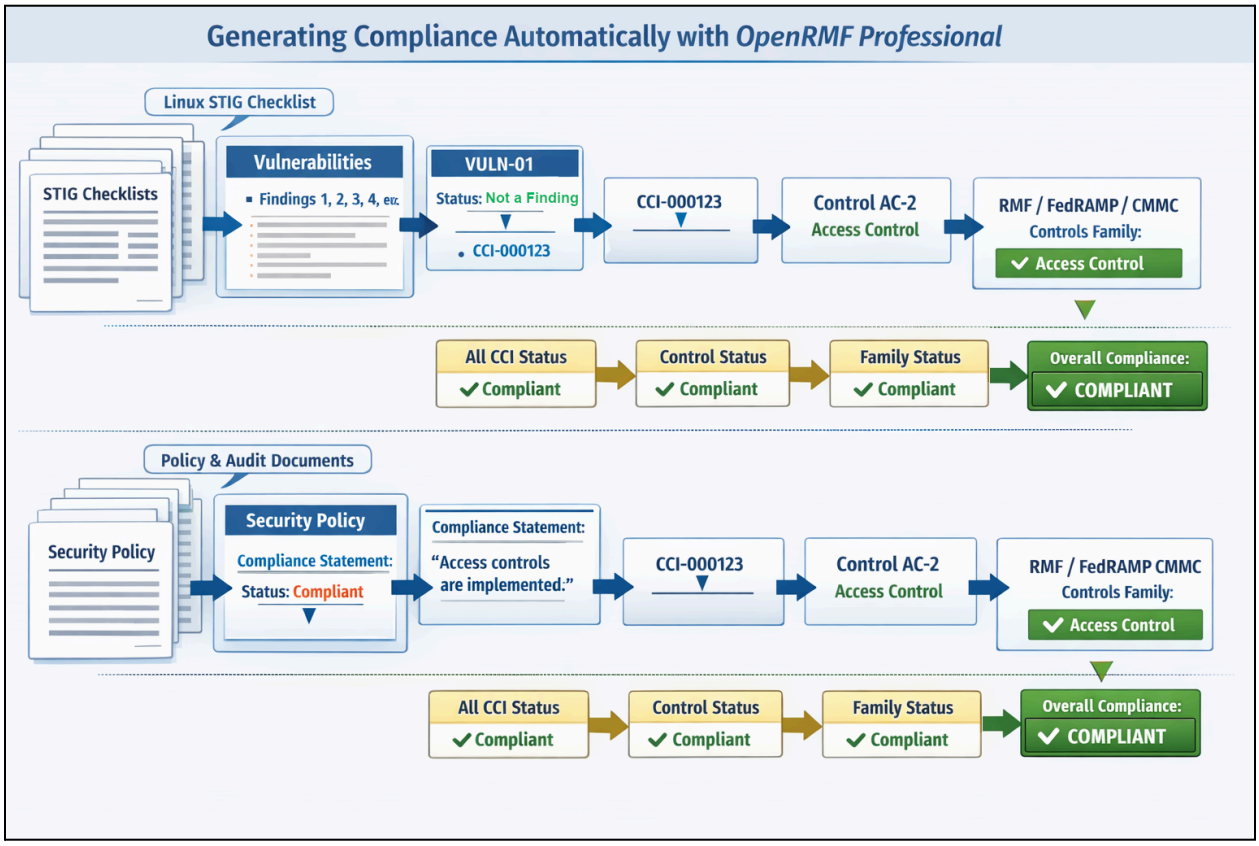
- Bulk editing of multiple vulnerabilities across all STIG checklists
- Bulk locking of vulnerabilities and checklists, for false positives and management
- Tracking of vulnerabilities in images and software containers
- Boilerplate checklists with predefined answers and status to standardize
- Ingestion of RapidFort image DISA Benchmark SCAP scans to checklists
- Full text searching of all checklist data using the included Elasticsearch stack
- Missing Checklist Wizard based on devices and their software bill of materials
- Track compliance history over time by accreditation, control family, and control



Compliance Generation Across Frameworks

With all data in one solution tracked and correlated, you can easily generate compliance at the framework level all the way down through control families and controls to the actual control correlation identifier (CCI) level. That lets you quickly run reports for RMF, FedRAMP, CMMC, ISO, or custom frameworks with filtering, overlays, and tailored controls in seconds across each of your accreditation packages in a structured way.

You also can track the history of your compliance over time as you generate updates throughout the life of your accreditation package. You can even extend an existing framework or even create your own cyber compliance framework with levels, controls and CCIs and track compliance with existing or custom checklists as well.



Essentially, OpenRMF® Professional absorbs raw security data, transforms it into actionable compliance insights, and supports decision-making and reporting — all while automating repetitive tasks that previously consumed your teams' time and attention.

Why It Works Well

OpenRMF® Professional provides the automation and centralization that compliance teams require to bypass the pitfalls of manual, siloed processes. There are several key reasons why this solution is the right solution for you and your organization.

Live Collaborative Environment

OpenRMF® Professional is a secure, web-based solution with role-specific views that empowers analysts, system administrators, developers, program managers, assessors, and directors to interact with real-time compliance data across their entire portfolios. Your team has specific roles and privileges within each individual accreditation package to only perform actions allowed. And the whole team has insight into their data, the impact their data has on the accreditation, and their part in the accreditation process as well. All viewable within a “single pain of glass”.

Configurable for Any Framework

Whether you need RMF, FedRAMP, CMMC, another defined framework, or even custom controls, OpenRMF® Professional supports frameworks with tailoring, overlays and sub-control granularity. It also has a way for you to use loaded frameworks, upload additional defined frameworks, and even create a framework with required levels, controls, and CCIs that you can use across all your accreditation packages.

Automatic Relationship Mapping

OpenRMF® Professional automatically correlates your checklist items to vulnerabilities, controls, and scan results — eliminating error-prone manual linkage. It does the same for all your compliance statements describing processes and procedures, as well as inherited or common controls. And does it at the control correlation identifier (CCI) level to show compliance at any framework level required.

Continuous Monitoring Built In

Automatic trend visualization and history tracking allows your teams to see vulnerability and compliance progress over time — a key requirement for continuous authorization and monitoring. You generate compliance automatically in minutes. And you track trends of compliance over time at a high level or even at a control or subcontrol level as well.

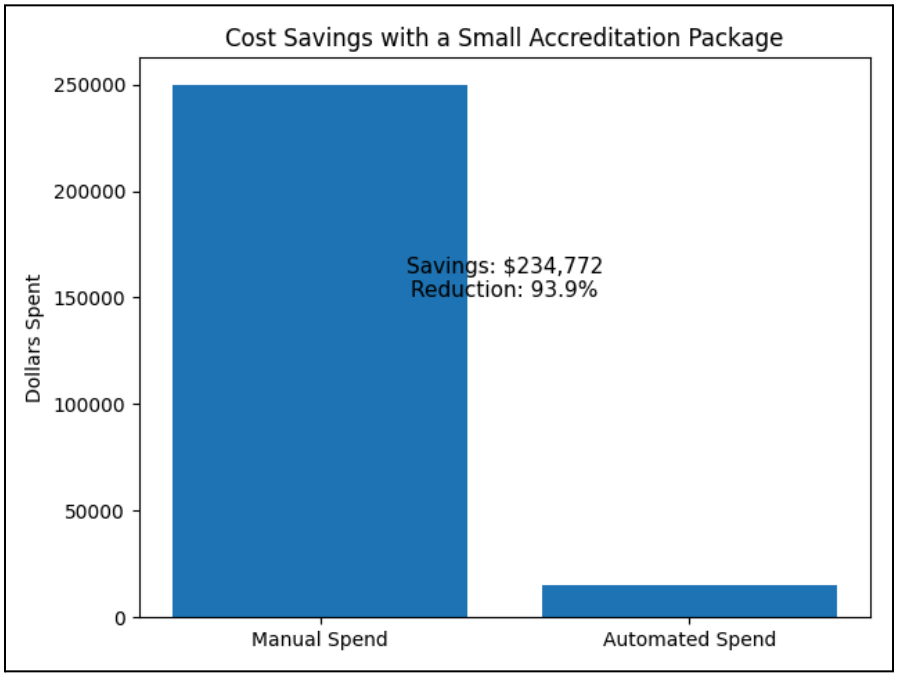
Time and Money Savings Results

Soteria Software internally tracks real usage metrics and customer feedback demonstrating OpenRMF® Professional's impact. With customers such as you tracking 508 ATOs with our solution at just 60% utilization of installations so far, we have over **$85M in estimated cost savings** attributable to time and money saved through automation. These are the immediate tangible benefits.

These figures reflect pervasive adoption across the US Department of War, US Federal and State environments, as well as contracting companies and commercial entities where compliance automation significantly improves team efficiency. We automate compliance with customers like you in the following areas:

- All 5 military agencies in the Department of War
- Other US federal and state agencies
- Top 50 Prime contractors and subcontractors
- Foreign Military Sales (FMS) customers

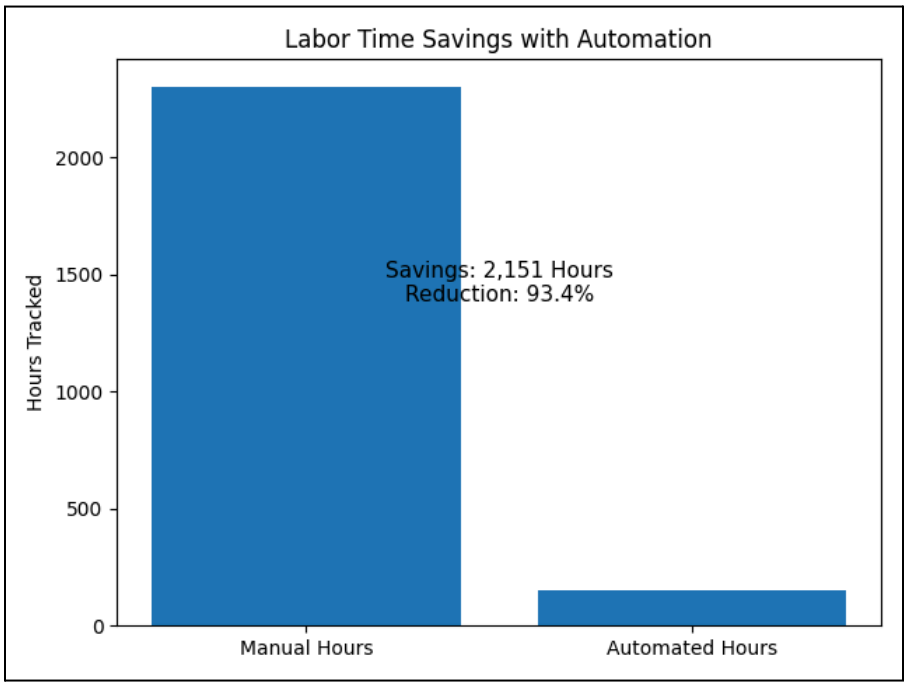
You can see below the positive results from using OpenRMF® Professional even on a small accreditation package of 20 devices in a single accreditation package (ATO). The amount of time and money saved is noticed in the 2nd month onward when customers use the online help, video on demand training included, and the intuitive web interface.



Your return on investment (ROI) is noticeable from there onward. And as more of your organization uses automation and collaboration, economies of scale enable even greater savings and standardization throughout the entire organization.

Not only do you see the tangible time and money savings through implementation of our solution. There are also intangible benefits as well that impact your team, your organization, and your security posture:

- More truthful data based on real scans
- Historical trends and analysis showing past, present, and future goals
- Structured data by type to allow assessors to do their job faster
- Live POA&M to show past work, mitigations, and remaining work to be done
- All interactively linked, live, and tracked historically automatically
- Less stressful employees that use the scans to automate the paperwork and artifacts



The time and money you can save can be calculated on your input at https://www.soteriasoft.com/resources/cybersavings.html. Use your own data to plug into our client-side-only sales calculator to see the true tangible benefit for you and your team when you automate your cyber compliance.

Conclusion

OpenRMF® Professional addresses a current critical gap in cyber compliance operations: transforming **manual, fragmented, and error-prone compliance workflows** into **centralized, automated, and collaborative processes**. By unifying scan ingestion, checklist tracking, POA&M management, compliance generation, and reporting within a single platform, organizations achieve:

- Faster time to compliance for RMF/FedRAMP/CMMC ATO and Readiness
- Reduced risk and improved continuous monitoring
- Lower operational cost and quieter staff workloads
- Broader visibility and shared understanding of cyber posture across teams
- A simple pricing model
- A solution any IT person can install, maintain, and support
- Same application can run in the cloud, on-premise, hybrid, or air-gapped network

By replacing spreadsheets and disparate files with actionable, correlated data backed by automation and APIs, OpenRMF® Professional allows teams to *focus on cyber engineering and risk reduction instead of compliance housekeeping*.

For organizations that cannot afford manual compliance inefficiencies — especially in US Federal, US DoD/DoW, and enterprise environments — OpenRMF® Professional offers a practical, proven path to automation, collaboration, and measurable results.

See more at https://www.soteriasoft.com/ by using our Live Demo site, our savings calculator, or any number of our videos and articles to see how we can help you and your team automate your cyber compliance.

As we say at Soteria Software:

Do The Work. Automate The Paperwork! ®

About Soteria Software

Soteria Software creates cyber compliance automation software. Using the right technologies for the right purpose, we enable reduction of task-based work around accreditations and ATOs up to 90%.

Our passion is to change the expectation for the world around cyber compliance – to expect hyperautomation, giving you and your team the time, energy and resources for proper cyber hygiene and improved cyber security.

The amount of data to collect, track, analyze, and report is more and more overwhelming. Which means automation must come into play to allow confidence and trust to permeate the process. And de-stress the directors, managers, staff, assessors, and government officials at the same time.

This has been the conversation with us (the owners of Soteria Software) since 2004 when we met at the Navy EOD TechDiv in Indian Head, Maryland. For the next 14 years we kept doing the same thing over and over and saying "there has to be a better way"! And no one solved this growing problem. So in the summer of 2018 we started working on what has become OpenRMF® Professional! We started with a simple STIG checklist viewer and editing with OpenRMF® OSS. And innovated from there forward.

Now we have added functionality, APIs, an improved user interface, AuthN/AuthZ, additional scan imports, integration with task management software, updating STIG checklists, bulk editing and locking operations, and more. We were constantly asked for more and more features and saw a need for not just an open source OpenRMF® OSS. We saw a need for the larger organizations, agencies, and even commercial companies to track revisions, merge scans, track your POA&M, and perform continuous monitoring.

Our OpenRMF® Professional solution is designed to use your compliance, patch, and vulnerability scans from the ground up. Automate around the data you already need to have. And do so in an automated fashion to make a Live POAM, generate compliance snapshots, track history and configuration management of your data, run data calls, and hyperautomate with our API as part of your larger Cyber Security Mesh Architecture (CSMA).

This company, Soteria Software, was created to fill that need and innovate the cyber compliance landscape around OpenRMF® Professional and more.