Cybersecurity Audit Automation

Summary of Roundtable, hosted by ATARC in November 2022

WHITE PAPER

Threats to IT systems are becoming increasingly complex and sophisticated, ranging from hacker attacks and insider threats to accidental data loss or damage to data. In order to ensure strong system security, audits are vital to eliminate potential gaps in security infrastructure and strategy. Due to growing cybersecurity infrastructure and increasingly sophisticated cybersecurity threats, continuous monitoring of information security systems through automation is the best way to accurately assess vulnerability across a complex threat landscape.

Both public and private sectors have much to gain from enforcing ongoing IT security auditing by automated processing. However, continuous monitoring of information security systems has several challenges to address, including technology, governance, controls evolution, data models, standardized frameworks, data sharing, and auditor evolution, just to name a few. Experts, thought leaders, and government leadership join in conversation at a recent roundtable discussion hosted by ATARC to share their thoughts about cybersecurity audit automation.

With many perspectives represented at the roundtable, this initial conversation centered on the different approaches to automating cybersecurity audits, and the various challenges the public and private sector are facing in this arena.

Government Perspective

Government agencies represented at the roundtable shared steps they are taking towards cybersecurity automation. All mentioned that a lack of funding contributes to slow implementation. With more staff, agencies would be able to more quickly standardize the data in NIST's Open Security Controls Assessment Language (OSCAL), which needs to occur before processes can be automated.

As defined by NIST, OSCAL is a "standardized, data-centric framework that can be applied to an information system for documenting and assessing its security controls". The goal of developing a standardized language is "to move security controls and control baselines from a text-based and manual approach to a set of standardized and machine-readable formats".

Other agencies remain focused on maximizing efficiencies with existing assets before introducing automation. Determining business objectives is key to understanding which tool is best aligned to automate internal processes and further the mission. Without proper budget, agencies cannot make progress with advanced cybersecurity objectives, let alone automation.

Still, other agencies are taking action on CIO priorities to automate security authorizations in a managed cloud environment. Through a fully automated deployment methodology, agencies can stand up new applications in the environment, and technical controls will automatically test processes and variables based on certain values. Staff can easily see the results of the automatic testing and quickly locate any found vulnerabilities. This approach is also scalable to the shared service level.

From an oversight perspective, agencies work to ensure issues are fixed in a timely manner, and that controls are continuously working as intended. While agencies will often have plans to fix issues identified in audits, plans are usually pushed to the side in favor of more urgent issues and are never executed. With continuous monitoring, auditors can more easily determine what fixes worked in the past, and what might continue to work based on historical data.

Business Perspective

Several private companies offering automation solutions were represented at the roundtable; however, each one took a different approach to addressing the challenges presented by cybersecurity automation. Each representative described

 info@atarc.org

a unique challenge government agencies experience with cybersecurity automation, and how these challenges can be solved through various strategies, approaches, or software.

- Expanding on the need for historical data, agencies and contractors must look at the issue in totality, and avoid binary decisions based on compliance rules. To efficiently connect OSCAL to separate processes, like automated configuration management, or hardening to validation testing, agencies need the context of past experiences across all of government to make better informed decisions.

- There are tools available that use OSCAL to automate entire assessment and authorization processes, from the conception of the system security plan through to the testing of actual controls and generating system assessment reports. ATARC's Cloud Security Working Group published their report in March 2022, which demonstrated assessment and authorization (A&A) in the context of a live SaaS system implementing an application developed and operated from a Blue-Green DevSecOps environment.

- Bringing industry best practices into the folds of government is a critical role of vendors. One such best practice is the use of security automation frameworks, which are a collection of tools to manage everything from the development process to hardening content that can be reused by different agencies. Instead of re-hardening content multiple times, the process is automated.

Still another best practice introduced to government is the use of InSpec profiles to conduct assessments independent from the hardening process. This allows agencies to determine whether systems are ready to go live, and can be run as a part of a DevSecOps pipeline.

Automating security in this way, a security expert is not needed at every step of the development process. To ensure this process is scalable, companies are developing a data standard to collect security testing results into a common data format in order for the data to be aggregated. The goal is to visualize and better analyze security data.

- Also available to government are open source, governance, risk and compliance (GRC) tools focusing on compliance documentation as code to generate and maintain system security plans (SSPs). It was noted that compliance is not cybersecurity, rather it's attestation and verification at scale. While agencies tend to focus on primary GRCs to automate processes, other areas outside of a primary GRC also require automation, but are difficult to accomplish with the single GRC tools available today.

- Tools are available to help simplify the Security Technical Implementation Guides (STIG) and Center for Internet Security (CIS) hardening process. The goal is to move agencies away from the historic 'fix and find' environment to one that is self-healing and compliant. Automating the hardening process removes most of the effort of building the quality upfront and the need for constant fixing.

- Other companies focus their efforts on helping other companies develop tools that are compliant with government standards. However, in certain instances, ensuring security can be more important than maintaining compliance. Automating security for the sake of compliance can cause greater issues, especially if problems identified in an audit are not addressed.

Audit Automation Challenges

To expand on the philosophy behind automation, one can think of automation in terms of tiers. The first element is baselining, where an agency identifies the problem and understands what the RFI is asking for. Unfortunately, vendors see agencies seeking zero trust solutions before addressing simple cyber hygiene issues. Taking a crawl, walk, run approach to risk management is recommended, especially with automation. Incrementally automating things over time using a specific governance framework will help with compliance.

Having an extensible framework for audit automation is key, however most agencies have one approach to each entity, whether it's Cloud AWS or GCP. Building a single approach to auditing these disparate environments is challenging, but even more challenging for auditors when examining how data is collected and inventoried. Certain tools are available to capture and automate all data components to aid in compliance auditing.

From a government perspective, it seems management has a tendency to downplay issues found in audits and convince governance groups why the issue does not need to be fixed immediately. There is often a challenge point between auditors and management, as auditors work to ensure issues get resolved whether the issue is a 'big' problem or not.

Agencies represented on the panel also cited a lack of collaboration as a central challenge to cybersecurity automation. Shifting priorities, whether due to political climate or business goals, make creating efficiencies across business units a challenge. Similarly, getting agencies to adopt practices, like threat scoring, to reduce baseline threats is a continual struggle.

Considered a fundamental challenge for auditors is the presence of significant bias. Currently, auditing is a very manual process with a massive gap in technology. There is no good way to centralize what audit logic should look like from a standardization standpoint in order to facilitate a neutral arbiter of truth. There needs to be a clear line of delineation between operational tools, internal security tools, internal compliance, management and what can be externally accessed.

Collaboration Recommendations

With many different vendors and perspectives represented at the roundtable, the question was asked: how do we cooperate and interoperate, so that we can effectively utilize all of our communities, but still enable business drivers?

Access to shared examples

The industry, nor government agencies, have access to a collection of archived system SSPs available to the public. The industry is hesitant to share examples of control or implementation statements, which is odd considering this is about security. An unwillingness to share information has always been a major obstacle in security automation, which does not exist in other fields where we see automation.

Understanding agency business objectives

Investing in a framework of how to approach the problem of security is critical for agencies to begin automation. However, the first step is to clearly define business objectives, and how to tie cybersecurity capabilities to those business objectives. Agencies and businesses alike need to understand what the business outcomes will be when implementing cybersecurity capabilities.

Improve education of automation and its benefits

While there may be certain agencies or groups still fearful that automation will replace jobs, representatives at the roundtable believe that may no longer be the case. Auditors are certainly clamoring for automated processes, and are eager for agencies to take steps towards identifying risk at scale. Moreover, with skilled tech labor in short supply, it's more unlikely certain careers are threatened by automation. However, educating non-tech workers on the basics of automation and the importance it has on business objectives is key to successful, and quick, implementation.

Changes to culture, structure, and processes

Many agencies are still structured for manual processes inhibiting their ability to automate. Using automation, certain tasks and groups may no longer be needed. As such, agencies must determine how to reorganize into a modern organization that functions on automation.

Address negative perception of audits

Vendors routinely bump up against agencies and workers who are fearful of audit findings and the methods auditors use to collect data. There is also concern with how operations could be impacted as a result of an audit. In general, there needs to be a fundamental mindset change of what findings are. Auditing as a continuous function is a very different process than a single audit in time. Continuous monitoring is now an integral part of operations and a way for issues to be found much more easily.

Include automation and automation for compliance in RFP scoring criteria

There are often vendors that come forward with system integrators and automation solutions but receive no points and are not selected for contracts. Agencies should review internal policies specifically around automation for compliance in order for RFPs to remain competitive in an ever-evolving technology landscape.