

# The Myths of Audit Automation

OSTENDIO



# Table of Contents

**We'll Cover**


1. Introduction
2. The 5 Myths
   - Myth 1: The Myth Of A Single View
   - Myth 2: The Myth Of Automatically Resolved Business Issues
   - Myth 3:  The Myth Of "Set It And Forget It"
   - Myth 4:  The Myth Of Automating Everything
   - Myth 5: The Myth Of One-Size Fits All
3. How These Myths Can Affect Your Audit
4. Deep Dive: The Myths And Soc 2
5. Automation Strengths
6. Conclusion


MALONEY + NOVOTNY LLC

**MALONEY + NOVOTNY**

is one of Ohio's largest full-service CPA and business consulting firms and celebrates 90 years of helping clients achieve their goals and financial success. The Firm provides attest, tax and advisory services through a long-term relationship built on trust and service. Maloney + Novotny is a member of Nexia International, a worldwide network of independent accountants, business advisors and consultants.



# Introduction

We hear a lot these days about automating compliance, particularly around the automation of compliance standards. The general impression given is that compliance is handled automatically when you configure the right automation of controls in your security program. But this cannot be further from the truth and, unfortunately, there is no "easy button" for preparing for and passing complex data security audits. Audits such as HITRUST, SOC 2, and NIST are challenging because they are built to show that, as an organization, you take security seriously.

Of course, automation itself is not necessarily a bad thing. The problem is the over-reliance on automation or the presumption that automation in itself can facilitate all your security and compliance needs. Correctly configured and relevant automation can save you time during an audit but, compliance work itself is invariably a cross-check against the overdependence on automation, which can fail for many reasons. **Errors with misconfiguration, broken connections, or a lack of familiarity with the purpose of automated controls can lead to significant security gaps in an automated program.** An over-reliance on automated processes can also lead to blind spots and a false sense of security. This blind faith can cost your company time and money and cause a distraction from the purpose of the initial audit. With the **average cost of a data breach** reaching $4.3 million in 2022, and a data breach in the healthcare industry averaging $10.10 million, organizations can't afford to be relaxed about data security.



As data security and audit preparation experts, we will evaluate some of the common myths we hear when talking to clients about complex data security audits and help you "bust" those myths and use automation in a way that benefits your business.



# The 5 Myths of Automation

Myths are a staple of society and gain traction through a combination of repetition and alignment with a desired or familiar narrative. A common myth you still hear today is that people once believed that the world was flat. Such a myth gets repeated to the point that it almost stands without objection. Logic and common sense bust this myth, but the myth continues regardless because it fits into a comfortable stereotype.

**So let's look more closely at some of the myths of audit automation and why these myths seem to endure despite logic and common sense telling us otherwise.**

## 1. The Myth of a Single View

Without the ability to compare with a consciously developed "What should be", how can any organization determine if they are operating as intended?

The purpose of an audit is described by Grant Elliott, Ostendio's founder and CEO, as comparing the "What is" in an organization versus the "What should be". In other words, comparing actual operational performance against the organization's goals, policies, and procedures. It is important to remember that every organization is different from its construction to its mission.

Therefore, implementing template policies and procedures verbatim will not accurately represent the operations of each company. That is not to say templates are not useful but they must only serve as a starting point to help you develop your policies and procedures - "What should be".

Unfortunately, many audit automation tools today come with a standard unconfigurable list of controls that don't let you independently define your policies and procedures. Instead, these tools pull in automated status indicators configured to show their perspective of the "What is". While that may have value, it is far short of what is required to operate an effective security program and is insufficient to complete a full security audit.

While there is value in automating the collection of evidence to demonstrate the "What is", to be effective from an audit perspective, this data must then be compared against the "What should be". In most cases, this requires manual intervention which many organizations overlook.

Given that so little of the process can be fully automated, it becomes challenging to provide a single view unless the GRC (governance risk and compliance) or IRM (integrated risk management) tool incorporates all the manual tasks and those that may be automated. An automation-only view will always fall short.

For example, within the Ostendio platform, some collection of evidence is automated, such as sending out policies to appropriate individuals to review every 12 months or training to be taken by employees as established by the user. In this instance, the use of automation for simple, but individualized reminder tasks take advantage of the time-saving element of automation without losing the integrity of the audit.

## 2. The Myth of Automatically Resolved Business Issues

Automation only reports status, it won't ensure a control is well-designed and effectively implemented.

Many organizations approach audit automation as the goal. Often this is because in smaller, less mature organizations security ends up falling into the domain of their IT leaders, and IT people tend to solve problems through technology. However well-intentioned, automation tools do not resolve most operational problems.

Don't fall into the trap of believing that you don't need a deep understanding of your business processes and associated controls. If a security or business leader implements an automated control without understanding its purpose, they will not be in a position to understand the impact or remediate the issue when it goes wrong. Instead, an IT leader should have a good understanding of your business, and the IT department and CISO should work together and understand the goals they are trying to achieve through automation.

An example might be automating the review of network logs. AICPA SOC 2 (2017) CC7.2 requires organizations to ensure mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures. There are many great SIEM (Security Information and Event Management) tools in the market today that help to shortcut this process. But it is important to realize that any tool is only as valuable as the logic behind the pre-configured automation. If the operator does not understand what they are looking at, it is likely they will miss

important alerts or waste time on false alarms. Audit automation tools that claim to pull logs in will never be as sophisticated as the specialist tools that are built for this purpose. So, the primary compliance challenge here is to ensure there is a clear process for how and which logs should be reviewed, and whether automated or not, a check must be in place to ensure this process is being followed and issues are identified.

Just as importantly, what is being done to remediate issues identified through monitoring? It is critical that action is being taken, and that an organization can demonstrate the occurrence and effectiveness of this action. None of this can be managed through simple automation or integration of an audit platform. Indeed, there is an entirely new generation of dedicated tools looking to solve this particular problem - SOAR (Security Orchestration, Automation, and Response) - but it's still very much in its infancy. And even today's SIEM tools still only cover a fraction of your environment. In an increasingly cloud-based business environment, sensitive data may be stored in multiple locations not covered by traditional SIEM tools, so an alternative process will still be required to monitor this data.

## 3. The Myth of Set It and Forget It

While the concept of "Set It and Forget It" is seductive, in practice it is a mistake to eliminate the human element with complete automation. Indeed, AICPA SOC 2 (2017) PI1.2 specifically requires organizations to check the validity of information inputs

Organizations tend to rely too heavily on automation which only reports on a control's status. It cannot automatically adapt and improve control design and implementation as the technology and threat landscape evolves. It is dangerous to "set it and forget it" because threat actors are not static, they are constantly adapting to increasingly effective technology.

For example, once the Target data breach was discovered, its security team learned everything that the hacker was able to do because they had a tool in place that was tracking the exploit. However, the breach happened in part because no one was monitoring the tool. They relied too heavily on technology to protect them and missed all the signs. The larger a company gets, the more complicated the environment becomes.

Additionally, technology is not perfect. APIs fail. When integration is not set up correctly, dashboards can show a false positive simply because an API transaction failed, and additional checks need to be put in place. Likewise, AICPA SOC 2 (2017) CC7.1 requires organizations to validate configurations through integrity checking of software and firmware. The SolarWinds breach highlights the need to be vigilant for unexpected scenarios that won't be picked up through traditional monitoring.

# 4. The Myth of Automating Everything

This may be why some cyber insurance firms that require SIEM technology, also require some manual intervention for clients to get coverage. Even when an audit automation tool has integrations with the security tools you use, this doesn't mean you have complete coverage.

Not everything can be or should be automated. While this will change and evolve, current technology only accounts for about 15-20% of a security audit. Activities like background checks, employee training, approvals, system configuration, purchasing, all require at least some degree of human participation. Even if you could automate everything, real-life processes are messy and while it may be simple enough to design the "happy path", you will spend so much time programming the exceptions, a well-documented manual or semi-manual process is often more efficient. Furthermore, when a process is too regimented, people start working around it or stop using it altogether. Think of cumbersome software approval processes resulting in shadow IT systems.

Examples of areas that can't be fully automated include Risk Assessments, Incident Response, and Change Management.

Other automation limitations include scope. Does an HR system integration cover all employees and contractors, including those based internationally? If not, then you need a two-tier process which may invalidate much of the advantage gained by setting the automation in the first place.

Integration with the tools you use also doesn't mean all elements of the control are covered. For example, the check mark in an employee background control may signify a background check was conducted but does not give the auditor the information to know why it was necessary, the scope of the background check, and what was considered to be an acceptable result. The essential context is missing when there is only a single green checkbox on an automation platform.

Furthermore, some actions require explicit approval, such as authorization, to access certain data, or confirmation that a process was completed as required. A good example here is change management where a requirement of AICPA SOC 2 (2017) CC6.8 for organizations to prohibit unauthorized changes unless organization-approved change requests are received.

## 5. The Myth of One-Size Fits All

Automation clients often discover that they lack certain controls and face the temptation to adopt the automation vendor's control set. However, doing so can present a problem. Your auditor must verify that all controls are implemented correctly. Auditors must also verify that the control implementation matches the policies and procedures, more "What is" does not lead to "What should be."

When it comes to audit preparation, a one-size approach does not fit all. Each business is different and has different data security requirements. Clients need a data security platform that can automate as necessary but also be configured to fit their data security needs.

Different organizations have different risk factors, from the data they retain, to the markets they service, the scale of their operation to their market prominence.



**AICPA SOC 2 (2017) CC4.1 requires organizations to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations. Applying a one-size fits all template does not meet this requirement.**



# Automation Strengths

None of this is to say that automation in itself is bad. Used appropriately, automation can drive significant operational efficiencies by pulling data into a central repository, scheduling tasks, issuing reminders, highlighting gaps, and calculating scores.

This type of automation can help make the process more efficient and effective. Combined with effective manual processes and procedures automation can be a powerful tool.

For example, the Ostendio platform provides the source of truth or the “What Should Be” making it easy for any organization to build out its policies and procedures in line with the organization’s unique construction and mission. In essence, the platform configuration becomes a reflection of the organization’s intended state and then allows you to compare that with the current status. This comparison and subsequent remediation are tracked and can be shown to the auditor so they can confirm the organization’s “what is” matches its “what should be”.

The Ostendio platform provides the source of truth or the “What Should Be” making it easy for any organization to build out its policies and procedures in line with the organization’s unique construction and mission.



# Conclusion

While the appeal of a single solution to automate your audit is understandable, the reality is, audits are challenging on purpose and require more than simple automation. Any platform you use should make it easier for the auditor to navigate the controls and drill down for supporting evidence as required. The auditor needs to be able to see that controls have been implemented deliberately ("what should be"), are being tracked against reality ("what is"), and that any discrepancies are being tracked and remediated. Technology can certainly support this process but it can't replace it.

A human element is required to prepare successfully for any complex data security audit and automation of appropriate alerts and reminders to key stakeholders can ease the burden of select audit tasks, but when it is overused organizations risk the cost of failing an audit and rebuilding a costly compliance program.


## Everyone Secure

Welcome to the next generation of security.

Ostendio is the only risk management platform that leverages the strength of your greatest asset. Your people. With deep customization, advanced intelligence, and flexible controls, you're always audit-ready, always secure, and always able to take on what's next.

**Schedule a demo today.**