Volume 1, October 2017

WHITEPAPER

FAREWELL TO AUDIT SEASON

by Nancy Free
Director of Audit, Compliance, and Risk
Armor Thought Leader

INTRODUCTION

I fondly remember a time when “Audit Season” was just that — a season. Once a year, auditors would appear – with and without fanfare - to thoroughly test our security controls. During their stay, companies would endeavor to provide the necessary evidence and details of their processes. Life during Audit Season is always a challenge for everyone involved. After all, audits are demanding. But it was a consolidated, one-and-done process. No matter how strenuous or time-consuming these audits became, we knew we were never far from that special day when the auditors completed their work and let us get back to ours.

It was a magical time. But it wasn’t meant to last.

Before too long, driven by improvements in technology and consumer protections, Audit Season became every day. And I mean Every. Single. Day. The list of compliance standards, and their hundreds of seemingly unique requirements continued to grow, placing a strain on tried and true compliance processes. Plus the level of rigor required by today’s audit firms only added to the weight of the entire affair.

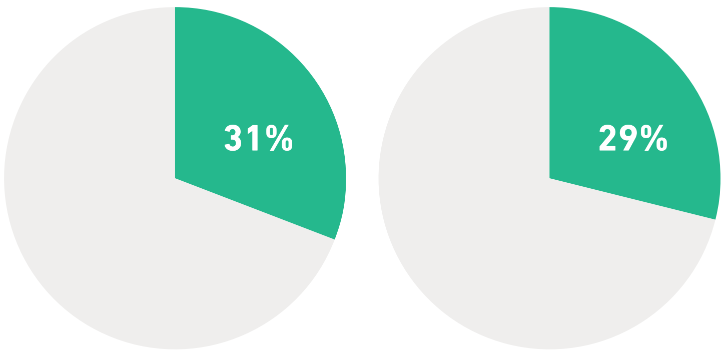
Some companies were fortunately able to identify this shift and adapt. They turned their compliance approach into a full compliance program by consolidating controls across multiple regulations and standards, optimizing and automating control execution wherever possible. Then they set forth developing a culture of compliance that would allow them to stay ahead of the curve. However, many, many more organizations were slow to respond, if at all. They sought to maintain most of the same processes and people that had carried them through audit seasons of yore. Leadership sounding something like “What’d we do last year?” and “Make that work again” is the chorus in the hallways.

It didn’t take long for their lives to devolve into fulfilling an endless stream of data requests from auditors, and listening to reminders from leadership on the importance of compliance attestation. Resources were regularly being pulled away from their core competencies, limiting productivity despite their best efforts to course correct. Caught in the momentum of maintaining compliance no matter the cost, they trudge on–and begrudgingly continue to do so every day.

> “These are the companies I want to reach with this white paper; those trapped in the cycle of never-ending compliance attestation.”

31% of CCOs do not know, or do not communicate, conduct and culture lessons across their organizations. Further, **29%** of CCOs have not documented, or do not know if they have, formalized compliance roles and responsibilities for their staff—it is foundational for employees to understand the importance of compliance and their role within the compliance structure.

Source: Stryker, Nicole. “The Compliance Journey: Boosting the Value of Compliance in a Changing Regulatory Climate.” KPMG. Ed. Karen Staines. KPMG LLP, 2017. Web. 13 July 2017.



TRAPPED BY SURGE COMPLIANCE

Surge compliance isn't an industry term, but it paints a necessary picture. Whether it's the constant burden of data requests, the lack of a defined, measurable, and repeatable approach to compliance or actual issues found during the audit, those affected are trapped by the momentum of becoming or staying compliant.

WHILE MOST OF THOSE AFFECTED CAN "MEET" THEIR COMPLIANCE REQUIREMENTS, THEY DO SO AT A GREAT COST IN TWO KEY AREAS:

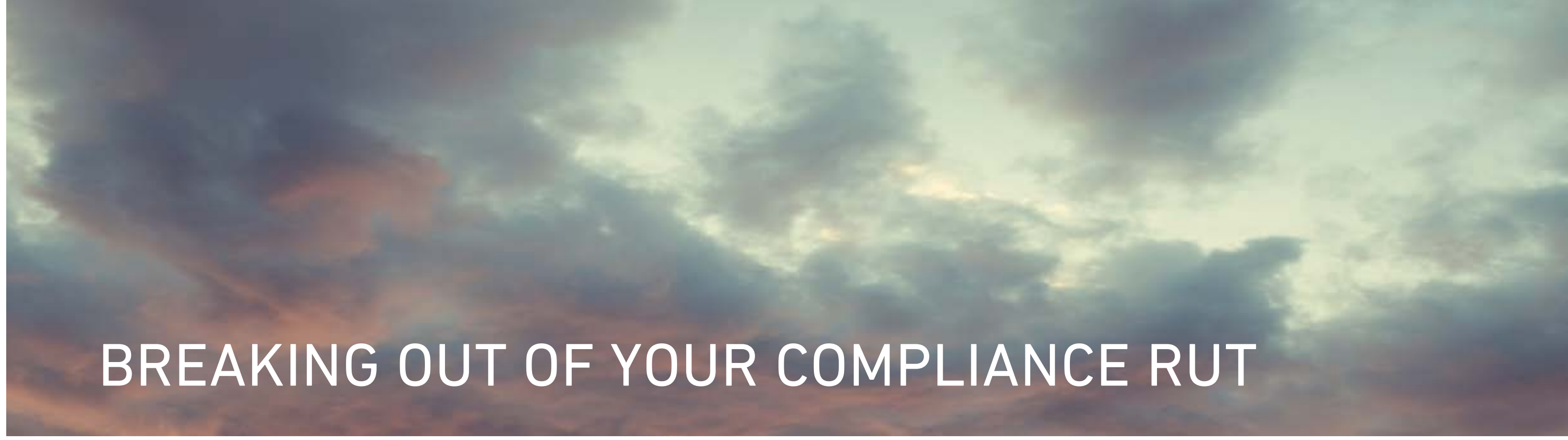
- Lost Productivity
- Diminished Company Morale and Overall Confidence

Lost Productivity

These companies suffer by not tapping the brakes on their daily operations or project schedules to address the needs of an audit. Since audits aren't planned with consideration to an employee's role and responsibilities, it's certain to serve as a distraction from the individual's regular workload.

Diminished Company Morale and Overall Confidence

This can be true of either company management which isn't seeing sufficient progress on key initiatives, or by audit firms who don't receive appropriate information from either undertrained or overwhelmed control owners. Frustrated and spent, those control owners may just decide that life is too short to put up with such pressure and leave that chaos behind, costing companies critical resources and knowledge.



BREAKING OUT OF YOUR COMPLIANCE RUT

Compliance attestation doesn't have to work this way. Of course, you may never again see those halcyon days of an Audit Season, **but you can at least break free of the surge and enact a continuous compliance program.**

Continuous compliance. I know those words may evoke a sense of dread for those caught up by surge compliance. However, in practice, the two couldn't be more different. Fundamentally, continuous compliance is the bridge over troubled waters and one that allows companies to understand and plan for the compliance challenges they may be up against.

This type of continuous program is something you drive within your own organization, not as a reaction to issues that auditors may identify during an assessment. It's not the side effect of simply having auditors at your door all the time.

To be continuously compliant means you're fully aware of how your policies, processes and operations stack up against all your relevant standards. It means that your staff knows – and more importantly UNDERSTANDS – what is expected, how those expectations are addressed day-to-day and how to measure the effectiveness of those requirements. In doing so, your people become empowered. They shed the ambiguity they once had and are now able to meet with your auditors as informed control owners who are able to drive those conversations. They can call BS when some junior auditor starts going off the rails in an interview, asking questions that are not relevant to the matter at hand. With a continuous compliance program, you're ensuring that you're ready for anything that is coming your way.

ENACTING CONTINUOUS COMPLIANCE

It sounds nice, doesn't it? Living in a state of perpetual readiness for an audit. It almost has a Zen quality to it. Now, I'm sure the too-good-to-be-true quality of continuous compliance elicited at least one scoff upon reading. And I completely understand that reaction. The cloud security industry, especially when it comes to compliance, is full of quick fixes and snake oil-like solutions. So, I won't take it personally if you're initially skeptical of this process. However, I can't stress enough that this is a very achievable process, and one that will pay dividends in the form of audit preparedness and reduced stress. Also, if you're stuck with surge compliance, what do you have to lose?

So, with that in mind, here are the seven steps to enacting continuous compliance. >>

Aggregate

Know your business and your customers' needs. What regulations or standards are each being held to achieving? How do those compare to one another?

- For example, the PCI DSS is often considered a good baseline standard of controls for an IT shop. While it may address the risks that credit card companies care about, it's not sufficient for a company that covers privacy issues. Healthcare records require some degree of privacy controls, but there are additional and more stringent controls needed ensure the protection of ePHI. The general IT controls needed to support Sarbanes-Oxley will not suffice for GLBA or ISO-27001 assessments.
- Third party providers must provide more and more proof of their diligence in cyber security and regulatory compliance. If you're a third-party provider, you should ask yourself if you're doing enough to meet the needs of your customers. If you're relying on a few of the standard certifications, like an AOC or a SOC2, but your customers must adhere to more strict requirements for FedRamp or HITRUST certifications, odds are you're not. In my experience, the standards we've been relying on to date are no longer sufficient to address the growing needs of regulators, and let's face it...we just want to make them happy and have them move along. Going forward, it will be the providers who take the time to consider and integrate their customers' needs into their own compliance program that will stand out as true partners. And that's a value add, no matter how you look at it.

Consolidate

Once you understand the needs of your business and your customers, consolidate those needs into a single control framework. Map the controls from all relevant frameworks against one another to better understand how performing an action once can achieve the requirements across many compliance standards. Tools can help with this, and many GRC tools on the market today offer this capability out of the box. For those in need of a more cost-effective approach, you can do this in Excel. Many of these mappings are already available online with a mere Google search standing between you and them.

Elevate

When you know the full population of needed controls, bubble them up to the more stringent requirement. By aiming for and achieving the higher standard, you'll be covered for all lesser standards too. This will be your baseline control framework. Next, assign control owners to the relevant areas. These individuals will ensure that controls are executed completely and accurately, day in and day out.

Calibrate

Ensure that your policies and procedures align with your new internal control framework. I find it helpful to include references within policies and procedures that tie into specific controls. This prevents updates from unknowingly impacting the control environment. It also helps you certify that you've addressed all controls within policy and that you can quickly and easily show an auditor where you specifically address a control.

Educate

In my experience, people want to do the right thing. Educate your control owners on continuous compliance, from how the framework came together, how periodic self-assessments will be required to make sure things work as expected (and if not, to bring that to light for remediation) as well as how this reduces the surge that comes with each audit. This will help the compliance team to gather evidence through the year that can be used when the auditors do come.

The Expectations for Your Team

Your controls are assigned to the appropriate teams with management level oversight, who integrate them into their day-to-day operations, policies and procedures. They perform periodic self-assessments to make sure their processes are working as intended. Keep in mind that these folks are not your internal audit team, but the people in charge of the actual execution of your processes. They will not write workpapers and document every infinite detail of how they ensure completeness and accuracy of the data they used. The intent here is not to turn your entire staff into auditors. Rather, it is to make these folks aware of the requirements they are facing in future audits and to provide them with the tools and processes needed to make sure they're ready.

> “I firmly believe that pain brings progress, and few things bring the pain like an audit can.”

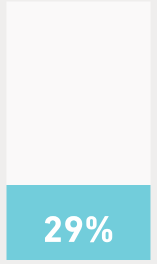
Innovate

I firmly believe that pain brings progress, and few things bring the pain like an audit can. However, as control owners begin to understand how performing a periodic self-assessment helps them find and fix issues as part of standard operations (saving them the drama of a risk exposure check during an audit and ample unplanned work), you'll find that they begin to take ownership of those controls. By doing so, they may become innovative. And trust me when I say, it's a beautiful thing when a control owner tells you “I don't want to have to review 200 people with access to this system. I'm going to just remove access to all but those who REALLY need it.” Why yes, that's a fabulous idea, and, not to mention the entire point of this control. Equally as endearing is the phrase, “You know, we have a tool in house than can be configured to look for non-compliance against these 10 controls. It's repeatable and we can show completeness and accuracy to our auditors!” Excellent! By all means, let's find ways to automate!

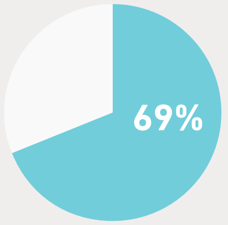
Administrate

This one is short and sweet. Continuous compliance requires diligent maintenance. Regular consideration of new control frameworks or regulations is critical to ensure your internal control framework is current and that you're keeping pace with your customers' needs.

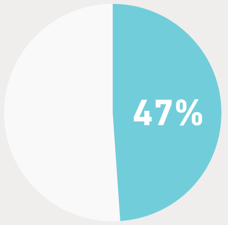
Once in place, this control set becomes your compliance bible. And like any well-written gospel, your controls should be in plain terms that most people understand. Here's why - auditors have their own language and terms. So do technologists. So do finance and accounting folks. Clarity and intuitiveness is key.



Only **29%** of organizations report that they assess compliance proficiencies and skills of their staff on an ongoing basis.



Only **69%** of CCOs say their organization leverages technology to support its compliance initiatives



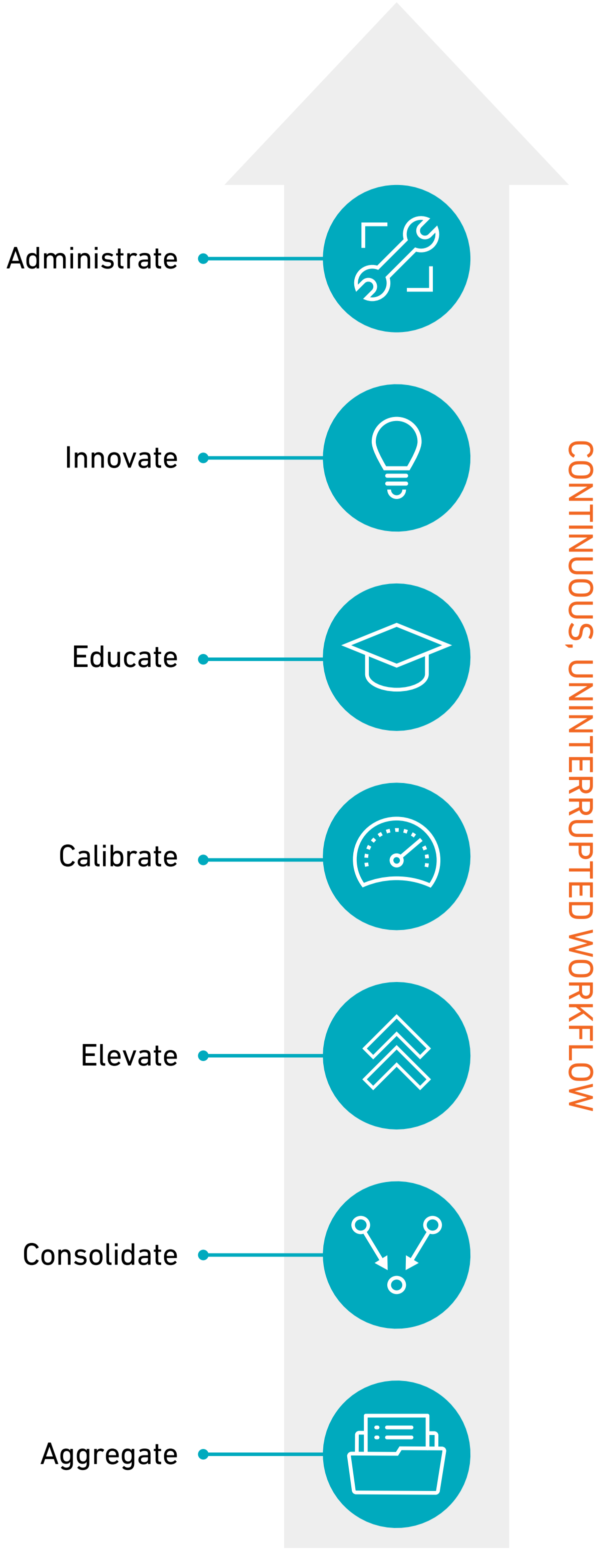
47% of CCOs say they use data analytics and other technology processes to conduct root cause and trending analysis.

Source: Stryker, Nicole. “The Compliance Journey: Boosting the Value of Compliance in a Changing Regulatory Climate.” KPMG. Ed. Karen Staines. KPMG LLP, 2017. Web. 13 July 2017.

Continuous Compliance in Action

This is continuous compliance. It means you're prepared. It means you can juggle not only the requests from your assessors, but also your projects and typical work assignments. Your team is on point and able to keep audits and auditors operating between the lines. And with all that marching along at a normal, operational cadence, you can begin to see those breaks between audit cycles.

Also, by regularly performing self-assessments, your control owners know the requirements. They have a thorough understanding of the threats they're responsible for mitigating. They also know how to prove that their processes are effective and they kick the tires on those processes regularly, by pulling data and validating their effectiveness. This creates a knowledgeable and effective control owner. And a team of those significantly boosts the confidence of any audit firm.



CONCLUSION

I'll be the first to admit that this process isn't perfect nor easy to implement. But, then again, no process is. And, certainly no process this advantageous should ever be expected to be "easy." It will require that you and your team become a finely tuned, no-nonsense continuous compliance machine. Which I know you can achieve – no matter your industry or current compliance status. This is the start to you escaping the chaos of surge compliance and taking back your processes and maybe a modicum of sanity.

So, now it's up to you. What are you waiting for? Audit Season is over and it's time for a fresh start.

Director of Audit, Compliance, and Risk
Armor

Nancy Free

- 20+ years of IT experience, including IT governance, risk, compliance, and audit.
- 15+ years in the IT Security field.
- Led IT and compliance teams in a variety of industries, including: energy, transportation, construction, mortgage lending, healthcare, and retail.

ARMOR™

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167