KRATOS®
READY FOR WHAT'S NEXT™

Tips to Reduce Cybersecurity Audit Fatigue

Tips to Reduce Cybersecurity Audit Fatigue

Audit Fatigue is Real

In this day and age, audit fatigue is a reality that must be recognized by both the auditing industry and the organizations undergoing audits. It can be quite frustrating for an organization's employees to provide evidence, and most times the same type of evidence, over and over again, multiple times a year. It can stifle employee morale and foster an "audit paralysis" mentality where getting audited is perceived as being an everyday thing, no end in sight, and takes away from employees focusing on core job functions. Another factor that comes into play for management is experiencing increased audit costs, further justifying the need to "re-think" audit scheduling timeframes.

Conducting audits is essential for organizations that are seeking to demonstrate compliance with various security frameworks. However, the process of conducting multiple audits can be exhausting and pull key resources away from other company initiatives, leading to what is commonly referred to as audit fatigue. Because each security framework (e.g., FedRAMP, PCI DSS, CMMC, HITRUST) has its own unique compliance requirements and annual assessment cycle, companies must dedicate critical company resources to support each audit. In this whitepaper, we explain the methodology that Kratos uses to reduce audit fatigue and streamline the process of validating compliance with multiple security frameworks.

1. Control Mapping – An Important Exercise

Knowing what controls and evidence from one compliance audit that can apply to another compliance audit(s) is the critical first step to reducing audit fatigue. Kratos applies this approach based on the type of audit, assessment timing, and evidence collection rules (i.e., when the evidence was collected, and "relevance" or "freshness" of the evidence).

As an experienced cybersecurity Third-Party Assessment Organization (3PAO), Kratos has mapped various control frameworks to one another to understand applicability and relationship, serving as a guide in helping our clients minimize the level of effort by leveraging evidence that addresses similar controls across different frameworks.

2. Identify the Minimum Baseline

After mapping common security controls across multiple compliance frameworks, the next crucial step is to identify the most prescriptive elements of security that the organization must demonstrate. This involves prioritizing requirements based on their level of stringency. By focusing on the most rigid elements of security, organizations can ensure that they are meeting and, in some cases, exceeding requirements across the cadre of compliance framework requirements.

Once the most prescriptive elements of security have been identified for a mapped requirement, organizations should develop a plan to demonstrate compliance. This may involve implementing standardized processes for demonstrating compliance with specific requirements and identifying standard, repeatable evidence. Demonstrating compliance is an ongoing process that requires regular monitoring and reporting. By focusing on the most prescriptive elements of security and identifying supporting evidence (e.g., screenshots, reports, policies, procedures, scripts, etc.), organizations can ensure that they are meeting their obligations across multiple compliance frameworks.

At Kratos, we work with our clients to identify the minimum baseline and support the globalization of controls in such a way that meets and or exceeds multiple compliance frameworks. Kratos' expertise in FedRAMP, PCI, CMMC, and HITRUST, as well as other federal and state requirements, allows us to form a global strategy for our clients' compliance needs.

3. Maintain a Historical Repository

One of the primary sources of audit fatigue is the need to track down evidence to demonstrate compliance to auditors. This can be a time-consuming and stressful process, particularly when dealing with multiple compliance frameworks. However, organizations can reduce this burden by maintaining a historical repository of evidence across mapped controls. This repository can serve as a roadmap for demonstrating conformance and can greatly simplify the process of validating compliance across multiple frameworks.

By maintaining a historical repository of evidence, organizations can reduce the amount of time and effort required to demonstrate compliance to auditors. Instead of having to track down evidence for each individual audit, organizations can simply refer to the repository to identify relevant evidence that has already been collected and stored. This can also help to ensure consistency in the evidence provided across multiple audits, reducing the risk of non-compliance and increasing the efficiency of the auditing process.

Overall, maintaining a historical repository of evidence is an important strategy for reducing audit fatigue and streamlining the process of validating compliance to multiple frameworks. By investing time in this up front, organizations will see compounded savings on valuable time and resources across each framework annually.

4. Know your Control Domains

While compliance frameworks may vary in their specific requirements, many share commonalities in terms of security requirements. These commonalities can be logically grouped into a reduced set of domains, which can generally be associated with non-overlapping stakeholders within the organization. By focusing on these commonalities, organizations can avoid duplicative efforts and reduce the burden of compliance across resources. On countless occasions, we have seen less prepared organizations assign resources to week-long audits, when a given individual may only need to participate for an hour or two over that entire week. If six people are in that week-long audit, it equates to 240 work hours, or 1 ½ months of otherwise productive time.

Kratos recommends aligning Control Domains to specific individuals. This not only establishes boundaries for leveraging resource time, it also ensures accountability and enables more focused discussions with appropriate personnel when they are actually needed. For example, most security compliance requirements fall into the following common domains. Most organizations can quickly read through this list and easily identify who is responsible:

- Access Control and Authentication
- Configuration Management
- Monitoring
- Logging
- Change Management
- Incident Management (including information security response)
- Release Management
- Software Development Life Cycle (SDLC)
- Vulnerability Management (Vulnerability Scanning, Anti-Malware, Risk Assessments, Intrusion Detection & Prevention)
- Information Security Policies and Procedures
- IT Technology Standards
- Boundary Protection
- Backups
- Business Continuity / Disaster Recovery
- Physical and Environmental Security

The goal of aligning staff to common audit domains is to save valuable resource time, which should be utilized to support the business. By aligning staff to common audit domains, organizations can avoid duplicating efforts and wasting employee cycles. This approach allows staff to become more efficient during audits, helping the organization to achieve its audit objectives in a timely and efficient manner.

Conclusion

Reducing audit fatigue takes partnership and collaboration between the auditor and the organization being audited. Working together, understanding control frameworks, and knowing how to map frameworks to shared common controls requires a "think-out-of-the-box" mentality. Finding the right dynamic is key and what separates Kratos from most auditing firms.

Kratos can map an organization's internal controls to multiple auditing frameworks and find ways to leverage evidence collected to simplify an organization's audit experience. This will help reduce audit expenses, improve employee morale, and decrease time spent on audit activities. Kratos can map an organization's internal controls to multiple auditing frameworks and find ways to leverage evidence collected to simplify an organization's audit experience. This will help reduce audit expenses, improve employee morale, and decrease time spent on audit activities.

About Kratos

Kratos has years of robust compliance and certification experience with government and commercial standards and compliance frameworks requirements. As one of the first and largest Federal Risk and Authorization Management Program (FedRAMP) 3PAOs, Kratos' compliance experience also includes CMMC (C3PAO), Payment Card Industry (PCI), Federal Information Security Management/Modernization Act (FISMA) and the National Institute of Standards & Technology (NIST) Risk Management Framework (RMF). Because of this experience, Kratos is viewed as a trusted compliance and governance partner by the Department of Defense (DoD), Federal Civilian Agencies, Intelligence Community (IC), and commercial organizations.

Contact us for a free consultation to see how we can serve your auditing needs.

By Joseph Scarzone – Manager, Cybersecurity Services

CyberSales@KratosDefense.com