**Lack of Automation in Managing Controls**

A common challenge that all organizations face is regulatory and policy compliance. In government agencies and highly regulated industries, compliance with a recognized framework of controls is mandatory. Additionally, all organizations have internal policy compliance requirements such as audits, business continuity, and disaster recovery.

Cybersecurity professionals across all industries are tasked with continuously evaluating and monitoring their information systems against the required set of security controls provided by these regulations.

In the federal space, agencies must adhere to NIST’s library of security controls and frameworks. For example, NIST SP 53-800, *Security and Privacy Controls for Federal Information Systems and Organizations*, is a catalog of security controls that is implemented via several federal security frameworks, including the NIST Risk Management Framework, the NIST Cybersecurity Framework, and FedRAMP.

Since its initial release, the number of security controls in SP 800-53 has climbed from less than three hundred to nearly a thousand, making it nearly impossible to manually manage compliance with them.

In addition, CSPs modify their offerings over time in response to customer requests and market demand. This natural inclination to improve a product can lead to system changes that might take the offering out of compliance — a situation known as configuration drift.

Compounding the risk of configuration drift is the fact that the controls themselves are occasionally updated. Each time there is an update to SP 800-53, for example, the system test plan must be updated to reflect those changes, which can be significant from one revision to the next. The upcoming new version of 800-53 (Rev 5) will add two new control families and result in a total of 1,000 to 1,050 controls.

A further complication for cloud offerings is the shared responsibility model of security. As observed earlier in this paper, the cloud host provides security *of* the cloud, whereas the CSP is responsible for the security of their offerings *in* the cloud. This makes it imperative that the CSP be aware of the controls under its management and be able to ensure compliance with them even when making improvements to their offerings.

Without automated and continuous controls management, a cloud offering is in constant jeopardy of falling out of compliance with the security controls it must follow in order to be used by federal agencies and other regulated organizations.