CONTINUOUS MONITORING

Managing Assessment Costs – Part 3 of 3

ABSTRACT

Continuous Monitoring is going to drive up the cost of compliance through a dramatic increase in the number of security control assessments. The third and final part of a three-part series of white papers on Continuous Monitoring, this white paper provides strategies and tactics you can use to manage this potentially explosive increase in assessment costs.

Part 1 in this series covered an introduction and brief history of Continuous Monitoring, along with common misconceptions and varying definitions. Part 2 of this series addressed monitoring strategy, including the frequency and method of assessments.

September 2014

RSA WHITE PAPER

Part Number H13429

TABLE OF CONTENTS

INTRODUCTION

From 2011 to 2013, the federal government saw several failed legislative attempts to mandate continuous monitoring (CM) for federal information systems. Interestingly, at the same time, there was also recognition within the information assurance (IA) community that CM was necessary and growing acceptance that a mandate for CM would eventually happen. In November 2013, the Office of Management and Budget (OMB) released Memo 14-03, which essentially provided that mandate with some ambiguity, including stipulation for partial or minimal CM capabilities and allowance of several years to implement these capabilities. OMB has also repeatedly stated that it is updating the circular A-130 to require CM. This movement by OMB certainly marks the beginning of the mandatory CM era.

While we all knew this mandate was coming, let's talk about the effect of mandatory CM. Simply put, CM will require control assessments at much greater frequency, which will require hiring or creation of more assessors and/or improved assessment capabilities. This has the potential to drastically increase the already bloated FISMA compliance budget, which is not realistically sustainable due to current federal debt and budget problems. This third and final part of the Continuous Monitoring white paper series will focus on methods for managing the cost of these additional control assessment costs.

CONTROL ASSESSMENTS: MORE AND MORE EXPENSIVE

CM equates to more assessments because they are performed more often. Until recently, federal Information Assurance (IA) compliance activities were conducted on a three-year cadence due in large part to OMB A-130, released in 1996, which stated that federal information systems were to be re-certified every three years. Depending on the Department/agency, this three-year cycle was conducted until the last year or two.

It was common until recently for most federal information systems to only have security control assessments performed once within that three-year period. There may have been an inspection, audit or significant change to the system that drove additional control assessments, but those were the exceptions.

How many more control assessments could be required with a CM mandate? An information system could realistically have 300 applicable controls which would have previously been assessed only once every three years, averaging 100 controls assessed per year. Keep this number in mind for the CM example to follow later.

Also keep in mind that "continuous" is a bit of a misnomer for CM. Following NIST Special Publication 800-137 which defines NIST's recommendations on CM, not all controls need to be assessed "continuously" but at frequencies that are appropriate on a per-control basis. NIST also says that theoretically each control can have a different assessment frequency, if it is appropriate for the environment and the organization. While no organization would ever actually assign a unique frequency to every control, the more likely scenario would be that groups of controls would be divided into a handful of frequencies. Taking the previous CM example, those same 300 applicable controls could break out into frequencies more like: 100 assessed annually, 50 assessed quarterly, 50 assessed monthly, 50 assessed weekly, 30 assessed every three days, and 20 assessed daily.

Number of Controls	Times Assessed in one year	Number of Assessments
100	1	100
50	4	200
50	12	600
50	52	2600
30	120	3600
20	365	7300
Total Number of Assessments per Year		14400

Table 1 -Example Number of Assessments

Compared with the old method, the total number of assessments under our example would be 14, 400 per year (Table 1). Only automated control assessments would be assigned such high frequencies as daily or every three days for things like vulnerability and configuration scans. Since these would be automated, they wouldn't add any real burden to the assessors under this new paradigm. However, subtracting those assessments (totaling 10,900) leaves 3,500 assessments that could be manual assessments. Compared with the previous model of 100 assessments per year, you would see an increase in assessments by 35 times!

The government is already spending over $1 billion per year on C&A/A&A assessments, while other compliance auditing requires an additional $1 billion – and this is before CM is implemented. Clearly, the challenge is how to perform many times more control assessments without increasing an already bloated compliance budget.

MORE CONTROL ASSESSMENTS WITH FEWER RESOURCES

There are several ways to reduce the costs of security control assessments, each of which will be covered briefly in this section. The goal is to accommodate many more assessments with the same or fewer resources.

Automated vs. Manual

To begin, automated assessments are obviously cheaper and faster than manual assessments. Assessments that use little to no human analysis or intervention reduce the assessment burden overall. Initially, it may take significant resources to implement the scanners/tools, and there is small overhead in managing these tools on an ongoing basis. Compared with manual assessments, the gain in number and frequency of assessments with automated assessments is enormous. However, the reality is that automating assessments provides only modest gains as a cost-saving tactic. This is because a majority of controls cannot be automated, so the controls which add the most to assessment costs will be the controls which require manual assessment.

The U.S. Department of Defense (DoD) is in the process of adopting NIST SP 800-53 as its control catalog and the rest of the federal community is already there. Therefore, looking at 800-53 as the example here, a large portion of those controls is process-oriented and will require manual assessment.

To automate as many control assessments as possible and maximize the benefits, the right tools are needed. SCAP-enabled scanners can streamline compliance checks using CVEs (common vulnerability enumerations) and CCEs (common configuration enumeration), and share their results with other reporting/management tools to show compliance. While buying new SCAP-compliant scanners and tools may sound like an expense rather than a cost savings, the elimination of costs for manual assessments -- especially considering the cost of third-party external assessors and the sheer scope of assessments -- would allow these tools to pay for themselves. In addition, because these scanners and tools have a finite useful life, they will need to be replaced over time anyway.

The automation of control assessments is important, but the technologies and protocols are maturing at different rates. The IA community and the vendors building the tools still need to agree on best practices and end-to-end workflows. In the meantime, another tactic to save money on assessments is to eliminate use of external assessors.

Develop Internal Assessment Capability

The question of how often to assess each control as part of a CM program is possibly the most important consideration. Table 2 contains guidelines for monitoring frequency. The frequencies were put together using several inputs. The criteria (automated/manual, critical, and volatile) were taken from NIST SP 800-137. These criteria were used to make the dimensions of the table. The physical limitations of automation were used to define the lower bounds of the frequency spectrum. It is accepted that an enterprise scan takes at least part of a day to run, setting the lower bound at one day.

The federal government has an enormous dependence on third party contractors, which is extremely expensive for short single-engagement audits/assessments. Building teams of internal assessors would be much cheaper in the long run. In the traditional C&A/ FISMA compliance model, it is very common for a federal organization to have an enterprise broken into dozens or even hundreds of information system (or sub-system) boundaries which need to be re-assessed every one to three years. In many cases, external assessors are brought in to assess each information system separately before respective authorizations expire. This activity can take anywhere from a few days to a few weeks at a cost ranging from $20k to over $100k, depending on the size and complexity of the system.

Considering a federal employee at a GS-13 pay rate typical for the skill level needed makes roughly $100k per year (and even doubling or tripling that amount for benefits and long-term pension costs), it is easy to see that even within the old paradigm of

less frequent assessments, use of internal assessors could save money. Now, factor in the additional flood of assessments that will be necessary as part of the new continuous monitoring paradigm, and it becomes critical to have an internal assessment team.

Even if internal assessors are not developed as federal employees, the short term engagements must be given up in exchange for a semi-permanent contractor team at the very least. While it is common practice to "pad" federal contract bids to safeguard against unknowns and to cover the overhead associated with the bidding process, the effect of this padding is amplified when applied to many small contracts. It would have much less effect on one long-term bid.

Common Controls

The concept of "control inheritance" or common controls must be leveraged to the greatest extent possible. Common controls allow a control to be assessed only once for the enterprise instead of repeating the assessment for every information system. Common controls have been called out for years as a mechanism for saving resources, but it can be done better.

Many opportunities for sharing common controls are missed due to lack of "big picture risk" insight. The C&A/A&A process is driven by individual system owners trying to get their authorization packages through the compliance process without regard for how it affects the rest of the enterprise. The Risk Executive role is growing in importance, as called out in the last revision of NIST 800-37. This is the type of role with visibility to know when and how information system owners and control owners can leverage each other's assessment data when they might not otherwise. This Risk Executive role assumes a level of maturity, however, that many organizations' security programs do not yet have.

The Right Frequency

One of the primary objectives of Part 2 in this white paper series is to illustrate the importance of assessing controls at the right frequency based on the sensitivity of the system and the volatility of the control itself. The point is to make informed risk decisions on assessment frequency and know when to say "no" to more assessments. An enormous amount of money and resources could be wasted by over-assessing controls that are unlikely to have changed during the assigned frequency or by assessing a non-critical system as often as a critical one.

The Right Methods

In the same way that you can save or waste money based on the frequency of assessments, the same is true for assessment methods. In the long run, not all assessments cost the same. For example, some controls assessments can be done asynchronously, such as "interview" method controls which can be answered by an email statement or attestation. In contrast, some controls demand live testing and might require multiple highly-paid system administrators and stakeholders to meet in real time. The effective cost difference between these two assessments is enormous, especially when multiplied over time across many information systems. The extra cost will sometimes be warranted, and sometimes not. Consider a scenario where a live test is recommended as the test method, but perhaps a screenshot or copy of a configuration file could be accepted in its place, if the system is less critical and does not require the highest level of assurance.

Cloud & Federal Risk and Authorization Management Program (FedRAMP)

The Federal Risk and Authorization Management Program (FedRAMP) provides essentially the same cost-saving benefits that common controls do. It is predicated on performing fewer assessments by sharing assessment results. FedRAMP is the authorization (C&A /A&A) process for cloud-based systems. The vendor or cloud service provider (CSP) pays the cost of assessing the controls. Presumably, federal customers will abandon some of their dedicated, onsite information systems and move that data to a cloud environment with similar capabilities.

The perception of savings can, in some sense, be a "shell game" because transferring the cost of assessing the controls to the vendor will mean, of course, an increase in what they charge for the cloud service. Ultimately, however, there are fewer controls being assessed than if every tenant/customer in the cloud environment was paying to do them individually at their respective sites. There is conceptually some savings going on, which would temper how much the vendor rolls into the cost.

Standardization of Technologies

Standardizing on a tool set across each Department or agency can save the federal government significant costs for acquisitions, maintenance and training. Standardization saves on the cost of assessments, as well. Furthermore, when discussing the standardization of tools used in assessments, savings are realized in both cases.

Consider the following: An assessor is assessing the control AC-02 from NIST SP 800-53 which concerns account management. The assessment is taking place in an environment where there are mainframes, Windows servers, Linux servers, local and network authentication and individual software application accounts. Each one of these represents a type of account, which begs a whole series of questions and interviews to fully satisfy the control. A single sign-on scheme can reduce this problem, but only for authentication related controls. Standardizing can solve this and many other problems. Assessing controls in a very heterogeneous environment means repeating every control assessment many times, to ensure that each control is implemented correctly on each platform. This requires more time and greater costs.

A 2013 report from the NASA OIG points out that they spent $26 million on 240 discrete purchases of IT security assessment and monitoring tools across nine control areas, with virtually no coordination between IA officials and for which existing software was already providing identical capabilities. A large portion of this was unnecessary software maintenance fees and unused software licenses. While this is also an acquisition issue, it is mentioned because the waste revolves entirely around assessment and monitoring software.

One final point on standardization as it pertains to assessments must be made. Manual assessments performed, on a group of 100 servers or 500 desktops, for example, will be done by sampling. The more standard servers or desktops are, the higher level of assurance that can be provided by smaller samples, that is fewer assessments.

Online/Remote Assessment

One last potential tactic is the use of online/remote assessments. This is an idea that has been around for a long time but has only recently gained ground in the federal space due to increased capabilities of secure tunnels, remote administration, remote monitoring and improved teleconferencing tools for interview-based assessments. This has the potential to lower costs for both external and internal assessors. External assessors can reduce overhead and charge less by eliminating travel expenses for their consultants. For internal assessors, an organization can leverage assessors from different sites. If Site A falls behind on assessments, Site B assessors can assist remotely when they have spare/idle time and vice versa.

SUMMARY

The number of control assessments that need to be performed will explode with mandatory Continuous Monitoring. There are many tactics to incrementally drive the cost of these assessments down. Plan ahead and use them strategically. They are mostly long-term responses that should be started immediately. They will provide assurance in the consistency and quality of the control assessment results and will keep assessment costs under control.