# CONTINUOUS MONITORING

## Monitoring Strategy – Part 2 of 3


## ABSTRACT

This white paper is Part 2 in a three-part series of white papers on the sometimes daunting subject of continuous monitoring (CM) and how to successfully manage a CM program. This paper addresses monitoring strategy, including the frequency and method of assessments.

Part 1 in this series covered an introduction and brief history of CM, along with common misconceptions and varying definitions. Part 3 of this series will cover strategies for managing assessment costs.

June 2014



RSA WHITE PAPER

Part Number H13181

## TABLE OF CONTENTS

# INTRODUCTION TO MONITORING STRATEGY

There are two issues essential to Continuous Monitoring (CM): how often should you perform control assessments, and by what methods? These represent the core differences between CM and the first ten years of FISMA compliance culture.

FISMA created a means for assessing and documenting information system risk, but was slow and expensive to update, resulting in documents that were frequently out of date. The desire for more current, accurate risk data and the ability to drive faster security improvements have been key drivers for CM.

All government agencies have at least begun to plan and budget for CM. Only a handful of the most forward-thinking agencies have tried to implement CM in earnest. The Department of Homeland Security (DHS) is actively working to fast-track the adoption of CM tools and processes by more federal Departments/agencies through two initiatives: Continuous Diagnostics and Mitigation (CDM) Program Tools and Continuous Monitoring as a Service (CMaaS). Through the CDM Program and specific CMaaS purchases, DHS is helping to remove technical hurdles in building CM solutions and processes on behalf of other federal entities.

If you are not in a position to wait for DHS to address your CM challenges or want to implement your own CM solutions, one of your first considerations should be how often to assess your controls and by what means.

## Control Assessment Methods and Frequencies

Previously, agencies who attempted to implement CM typically focused on a narrow band of controls, like vulnerability and configuration scanning which are easily automated and / or seem more critical than other controls. This is understandable since these types of assessments are “low-hanging fruit” and a logical place to start. Process-oriented controls, however, like policy-writing and personnel security have not received as much attention for CM.

While some controls may be considered less important, no controls are unimportant. There is no consensus on the frequencies and methods used for an effective and comprehensive continuous control monitoring strategy. While there are some written guidelines in the federal community, many of them are in draft.

SP 800-137 is NIST’s publication dedicated to CM. It describes the steps to develop a CM program and implement it. Of all CM documents, 800-137 spends the most time on the subject of manual control assessment as part of the CM scheme. It also includes a section on factors influencing the frequency of assessments in CM. Those factors will be covered below.

## Using SCAP for Automation

Another critical element to introduce before going any further is the Security Content Automation Protocol (SCAP). SCAP is a group of specialized XML formats called specifications. These specifications enable automation and information sharing and enable security tools to share scan data, analyses, and results. This is done by creating common taxonomies, language, and identifiers for IT products, configurations, and vulnerabilities. Common Platform Enumeration (CPE), for example, is an SCAP specification that uniquely identifies IT products, down to very subtle version differences. Common Vulnerabilities and Exposures (CVE) is a specification that tracks many thousands of unique vulnerabilities. Common Configuration Enumeration (CCE) uniquely identifies misconfigurations. SCAP defines the structure for grouping multiple specifications together, and using them to perform various scans and reports.

The point to take from this is that because of the common language element provided by XML and by SCAP, disparate tools and organizations can share data now where they couldn’t before, including high-volume, frequent scan data across huge ranges of hosts. The relevance of these facts to this paper is that SCAP had reduced obstacles in scanning and reporting workflow and so, has increased the frequency with which some scans can be performed. New methods for performing automated assessments are being created and improved upon due to these new SCAP technologies, and automation is a significant consideration as to the frequency of assessments.

## Controls Which Require Manual Assessment

Despite improvements in automation, a vast majority of the controls in NIST SP 800-53, the primary security control catalog for the federal government, cannot be assessed automatically. Policy and process-oriented controls, physical and personnel controls, and even many technical controls cannot be automatically assessed. The point of mentioning this is, like the SCAP consideration above, the level of effort to perform an assessment is an important consideration to how often it can and should be performed.

### Factors to Consider for Assessment Frequency

**Impact/Security Category.** One of the main factors to consider for defining the frequency of the control assessments is the criticality of the information system. This can be decided by the criticality from a Business Impact Analysis (BIA) or from the Security Category assigned according to FIPS 199 and using NIST SP 800-60. A system with a higher criticality or Security Category should have its controls assessed more often. A system with a lower criticality or Security Category should have its controls assessed less often.

**Automated vs. Manual.** The next factor should be whether the individual control is automatable or manual. Manual controls can likely not be assessed as frequently as automated controls. This is just a sheer logistical truth. A fixed amount of employees can only perform so many manual assessments in an allotted time. Automated controls, however, despite the potential for much higher frequency, should only be assessed as often as is useful. An enterprise patch scan may be run daily, for example. Running two patch scans a day would take twice the effort, but may not be twice as useful.

**Volatility.** A control that is known to change more often should be assessed more often. This means, for example, configuration checks should be assessed more often than a written policy, because the former would change much more often than the latter.

## ANALYSIS

Having introduced many variables, it is time to tie them together. The CM concept is useful and will be mandatory soon. Despite this, it is often vague, there are few requirements defined, and many of them that are, are still in draft. Some controls can be monitored by automated means, but most cannot. NIST SP 800-37 Rev 1 says that systems authorizations should define a monitoring strategy including the assessment frequency, but NIST does not recommend what the frequencies should be. Another critical piece that NIST does not define is how to correlate existing automatable processes to the passing and failing of specific NIST SP 800-53 controls for continual updating of system authorization documents like the System Security Plan (SSP). This paper cannot solve all of these problems, but can chip away and reduce the scope of the questions.

### Method: Manual vs. Automatic

The following table was created for this paper using references from NIST SP 800-53, 800-137, and CAESARS FE. It correlates control families from 800-53 to the 11 “automation domains” listed in 800-137 and CAESARS FE. The automation domains are groups of automated technologies which are, in turn, mapped to specific controls. For example, if the domains in the middle column, were implemented, the monitoring requirement for the controls in the right column would be at least partially satisfied.

**Table 1 - Correlating NIST 800-53 Controls to Automation Domains**

| NIST SP 800-53 Control Families | Applicable Security Automation Domains (per 800-137 / CAESARS FE) | Potentially Automatable Controls |
|---|---|---|
| AC - Access Control | Event Management | AC-4, Information Flow Enforcement; AC-17, Remote Access; AC-18, Wireless Access; |
| | Incident Management | |
| | Configuration Management | AC-2, Account Management; AC-3, Access Enforcement; AC-5, Separation of Duties; AC-7, Unsuccessful Login Attempts; AC-9, Previous Logon (Access) Notification; AC-10, Concurrent Session Control; AC-11, Session Lock; AC-19, Access Control for Mobile Devices; AC-20, Use of External Information Systems; AC-22, Publicly Accessible Content; |
| | Network Management | AC-4, Information Flow Enforcement; AC-17, Remote Access; AC-18, Wireless Access; |
| | Information Management | AC-4, Information Flow Enforcement; AC-17, Remote Access |

| | | |
|---|---|---|
| **AU - Audit and Accountability** | Event Management | AU-2, Auditable Events; AU-3, Content of Audit Records; AU-4, Audit Storage Capacity; AU-5, Response to Audit Processing Failures; AU-6, Audit Review, Analysis, and Reporting; AU-7, Audit Reduction and Report Generation; AU-8, Time Stamps; AU-12, Audit Generation; AU-13, Monitoring for Information Disclosure; |
| | Incident Management | |
| **CA - Security Assessment and Authorization** | Vulnerability Management | CA-2, Security Assessments; CA-7, Continuous Monitoring |
| | Patch Management | |
| | Event Management | |
| | Incident Management | |
| | Malware Detection | |
| | Asset Management | CA-7, Continuous Monitoring |
| | Configuration Management | CA-2, Security Assessments; CA-7, Continuous Monitoring |
| | Network Management | CA-7, Continuous Monitoring; |
| | License Management | CA-7, Continuous Monitoring; |
| | Information Management | CA-3, Information System Connections; CA-7, Continuous Monitoring; |
| **CM - Configuration Management** | Vulnerability Management | CM-3, Configuration Change Control; |
| | Patch Management | CM-3, Configuration Change Control; |
| | Configuration Management | CM-2, Baseline Configuration; CM-3, Configuration Change Control; CM-5, Access Restrictions for Change; CM-6, Configuration Settings; CM-7, Least Functionality |
| | Asset Management | CM-2, Baseline Configuration; CM-3, Configuration Change Control; CM-4, Security Impact Analysis; CM-8, Information System Component Inventory |
| | Network Management | CM-2, Baseline Configuration; CM-3, Configuration Change Control; CM-4, Security Impact Analysis; CM-6, Configuration Settings; CM-8, Information System Component Inventory; |
| | License Management | CM-8, Information System Component Inventory; |
| | Information Management | CM-7, Least Functionality; |
| **IA - Identification and Authentication** | Configuration Management | IA-2, Identification and Authentication (Organizational Users); IA-3, Device Identification and Authentication; IA-4, Identifier Management; IA-5, Authenticator Management; IA-8, Identification and Authentication (Non-Organizational Users) |

| | | |
|---|---|---|
| | Vulnerability Management | |
| | Patch Management | |
| | Event Management | |
| | Incident Management | IR-4, Incident Handling; IR-5, Incident Monitoring; |
| | Malware Detection | IR-5, Incident Monitoring |
| **IR - Incident Response** | Configuration Management | IR-5, Incident Monitoring |
| | Vulnerability Management | MA-2, Controlled Maintenance |
| | Patch Management | MA-2, Controlled Maintenance |
| **MA - Maintenance** | Configuration Management | MA-5, Maintenance Personnel |
| **PE - Physical and Environmental Protection** | Configuration Management | PE-3, Physical Access Control |
| | Vulnerability Management | |
| | Patch Management | RA-5, Vulnerability Scanning |
| | Event Management | |
| | Incident Management | |
| | Malware Detection | RA-3, Risk Assessment |
| **RA - Risk Assessment** | Configuration Management | RA-3, Risk Assessment |
| | Vulnerability Management | |
| | Patch Management | SA-11, Developer Security Testing; |
| | Software Assurance | SA-11, Developer Security Testing; SA-12, Supply Chain Protection; SA-13, Trustworthiness; SA-14, Critical Information System Components; |
| | Malware Detection | SA-12, Supply Chain Protection; SA-13, Trustworthiness |
| | Asset Management | SA-10, Developer Configuration Management |
| | Configuration Management | SA-7, User Installed Software; SA-10, Developer Configuration Management |
| **SA - System and Services Acquisition** | License Management | SA-6, Software Usage Restrictions |
| | Event Management | |
| | Incident Management | SC-7, Boundary Protection; |
| | Network Management | SC-2, Application Partitioning; SC-5, Denial of Service Protection; SC-7, Boundary Protection; SC-10, Network Disconnect; SC-32, Information System Partitioning; |
| **SC - System and Communications Protection** | Information Management | SC-9, Transmission Confidentiality; |

| | | |
|---|---|---|
| **SI - System and Information Integrity** | Vulnerability Management | SI-2, Flaw Remediation; SI-11, Error Handling. |
| | Patch Management | |
| | Event Management | SI-3, Malicious Code Protection; SI-4, Information System Monitoring; and SI-7, Software and Information Integrity. |
| | Incident Management | |
| | Software Assurance | SI-11, Error Handling |
| | Event Management | SI-4, Information system Monitoring |
| | Incident Management | |
| | Malware Detection | SI-3, Malicious Code Protection; SI-4, Information System Monitoring; SI-7, Software and Information Integrity; and SI-8, Spam Protection. |
| | Configuration Management | SI-2, Flaw Remediation |
| | Network Management | SI-4, Information System Monitoring |
| | Information Management | SI-12, Information Output Handling and Retention |
| | Software Assurance | SI-13, Predictable Failure Prevention |
| | | |

This table above represents ~64 controls that NIST suggests may be automatable, but it is unclear whether all/some/none of the enhancements of each of these controls are included. Enhancements are variants of the control that count as separate controls. Even assuming that some of the enhancements are applicable, even doubling the count only goes up to ~128, or tripling them drives the count to less than 200, out of roughly 900 controls in the latest revision of 800-53.

Taking all of these things into consideration, saying 200 controls could be assessed by automated means would likely be a high estimate due to several issues:

- The first is an issue covered in Part 1 of this series in the section called "Automating the Protection ≠ Automating the Assessment of Protection." The list of "automatable" controls is a mixture of controls which can be 1) implemented by automated means and/or 2) assessed or monitored by automated means, and for CM we are only talking about the latter.
- Next, the number of candidate controls whose assessment may be automatable is even further reduced by the fact that not every organization has every scanner or sensor to perform some of the assessments.
- Finally, the number is reduced again by the fact that with some controls are written with compound requirements, and only a portion of the control can be automated.

There are four entire families of NIST SP 800-53 that do not appear anywhere in Table 1: AT - Awareness and Training, CP - Contingency Planning, MP - Media Protection, and PS - Personnel Security Planning. This means they have no connection to an automation domain and all of the controls for each of these four families must be assessed manually. In addition, for each family that is in the table, only a subset of the controls is listed. Every control for each of those families that is not listed must also assessed manually.

To summarize this section, using the best guidance available from NIST and DHS, we cannot arrive at an explicit list or specific count of controls that are automatable. We can, however, with some certainty, scratch 700-800 controls off of that list, which is a good start.

## Assessment Frequencies: How Often is "Continuous"?

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.

Since OMB A-130's criterion for once-every-three-year assessment has been rejected as too infrequent, the upper bound must be less than three years. Many IA reviews occur annually with no problems, so annually becomes an acceptable upper bound for

our spectrum, providing the system it applies to is not particularly critical. Therefore, all of the frequencies, from the best-case to worst-case scenarios, must fall between one day and one year. The rest is just working out the increments and permutations, using three previously-mentioned assumptions:

- Manual assessments will be less frequent than automated
- Critical systems will be assessed more than non-critical
- Volatile controls will be assessed more frequent than non-volatile.

**Table 2 – Recommended Assessment Frequencies**

| | **Critical Systems** | | **Non-Critical Systems** | |
|---|---|---|---|---|
| | **Volatile Controls** | **Not Volatile Controls** | **Volatile Controls** | **Not Volatile Controls** |
| **Automated** | Daily – every few days | Weekly - Monthly | Weekly – Bi-weekly | Quarterly - Annually |
| **Manual** | Weekly - Biweekly | Monthly - Quarterly | Monthly - Quarterly | Annually |

## SUMMARY

The Continuous Monitoring paradigm will require a much larger number of control assessments. While automation is one of the first things people think of when the subject of CM comes up, a relatively small percentage of the controls can be assessed by automated means. Deciding on the right assessment frequencies for control assessments is of critical importance. Under assessing fails to provide the insight that is the core intent of the CM movement. Over assessing can quickly squander massive resources with no improvements in security.

To read more about managing the cost of the control assessments, please refer to the third and final part of this series.