Chapter Two: Continuous Monitoring

2. Continuous Monitoring

2.1. Introduction

A critical aspect of managing risk to information from the operation and use of information systems involves the continuous monitoring of the security controls employed within or inherited by the system. Conducting a thorough point-in-time assessment of the deployed security controls is a necessary but not sufficient condition to demonstrate security due diligence. An effective organizational information security program also includes a rigorous continuous monitoring program integrated into the System Development Life Cycle (SDLC). The objective of the continuous monitoring program is to determine if the set of deployed security controls continue to be effective over time in light of the inevitable changes that occur. Continuous monitoring is a proven technique to address the security impacts on an information system resulting from changes to the hardware, software, firmware, or operational environment. A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to organizational officials in order to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the information system. Continuous monitoring programs provide organizations with an effective mechanism to update *Security Plans*, *Security Assessment Reports*, and *Plans of Action and Milestones (POA&Ms)*.

An effective continuous monitoring program includes:

- Configuration management and control processes for information systems;
- Security impact analyses on proposed or actual changes to information systems and environments of operation;
- Assessment of selected security controls (including system-specific, hybrid, and common controls) based on the defined continuous monitoring strategy;
- Security status reporting to appropriate officials; and
- Active involvement by authorizing officials in the ongoing management of information system-related security risks.

2.2. Purpose

The purpose of this chapter is to establish and define how Continuous Monitoring will work in a cloud computing environment and specifically within the FedRAMP framework. This document will also serve to define reporting responsibilities and frequency for the Cloud Service Offering Service Provider (CSP).

2.3. Background

Service Provider is required to develop a strategy and implement a program for the continuous monitoring of security control effectiveness including the potential need to change or supplement the control set, taking into account any proposed/actual changes to the information system or its environment of operation. Continuous monitoring is integrated into the organization's system development life cycle processes. Robust continuous monitoring requires the active involvement of information system owners and common control providers, chief information officers, senior

information security officers, and authorizing officials. Continuous monitoring allows an organization to: (i) track the security state of an information system on a continuous basis; and (ii) maintain the security authorization for the system over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and represents a significant change in the way security authorization activities have been employed in the past. Near real-time risk management of information systems can be accomplished by employing automated support tools to execute various steps in the Risk Management Framework including authorization-related activities. In addition to vulnerability scanning tools, system and network monitoring tools, and other automated support tools that can help to determine the security state of an information system, organizations can employ automated security management and reporting tools to update key documents in the authorization package including the security plan, security assessment report, and plan of action and milestones. The documents in the authorization package are considered "living documents" and updated accordingly based on actual events that may affect the security state of the information system.

2.4. Continuous Monitoring Requirements

FedRAMP is designed to facilitate a more streamlined approach and methodology to continuous monitoring. Accordingly, service providers must demonstrate their ability to perform routine tasks on a specifically defined scheduled basis to monitor the cyber security posture of the defined IT security boundary. While FedRAMP will not prescribe specific toolsets to perform these functions, FedRAMP does prescribe their minimum capabilities. Furthermore, FedRAMP will prescribe specific reporting criteria that service providers can utilize to maximize their FISMA reporting responsibilities while minimizing the resource strain that is often experienced.

2.5. Reporting and Continuous Monitoring

Maintenance of the security Authority To Operate (ATO) will be through continuous monitoring of security controls of the service providers system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to FedRAMP per the schedules below. The submitted deliverables provide a current understanding of the security state and risk posture of the information systems. They allow FedRAMP authorizing officials to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. The deliverable frequencies below are to be considered standards. However, there will be instances, beyond the control of FedRAMP in which deliverables may be required on an ad hoc basis.

The deliverables required during continuous monitoring are depicted in Table 2: FedRAMP Continuous Monitoring . This table provides a listing of the deliverables, responsible party and frequency for completion. The table is organized into:

- **Deliverable** – Detailed description of the reporting artifact. If the artifact is expected in a specific format, that format appears in **BOLD** text.
- **Frequency** – Frequency under which the artifact should be created and/or updated.

206 • **Responsibility** – Whether FedRAMP or the Cloud Service Provider is responsible for
207 creation and maintenance of the artifact.

Deliverable	Frequency	Responsibility		
		FedRAMP		Cloud Service Provider
Scan reports of all systems within the boundary for vulnerability (Patch) management. **(Tool Output Report)**	Monthly			✓
Scan for verification of FDCC compliance (USGCB, CIS). **(SCAP Tool Output)**	Quarterly			✓
Incident Response Plan.	Annually			✓
POAM Remediation **(Completed POA&M Matrix)**	Quarterly			✓
Change Control Process	Annually			✓
Penetration testing **(Formal plan and results)**	Annually	✓		✓
IV&V of controls	Semi-Annually	✓		
Scan to verify that boundary has not changed (also that no rogue systems are added after ATO) **(Tool Output Report)**	Quarterly			✓
System configuration management software **(SCAP Tool Output)**	Quarterly			✓
FISMA Reporting data	Quarterly			✓
Update Documentation	Annually			✓
Contingency Plan and Test Report	Annually			✓
Separation of Duties Matrix	Annually			✓
Information Security Awareness and Training Records Results)	Annually			✓

208 **Table 2: FedRAMP Continuous Monitoring Deliverables**

2.6. Routine Systems Change Control Process

The Change Control Process is instrumental in ensuring the integrity of the cloud computing environment. As the system owners as well as other authorizing officials approve changes, they are systematically documented. This documentation is a critical aspect of continuous monitoring since it establishes all of the requirements that led to the need for the change as well as the specific details of the implementation. To ensure that changes to the enterprise do not alter the security posture beyond the parameters set by the FedRAMP Joint Authorization Board (JAB), the key documents in the authorization package which include the security plan, security assessment report, and plan of action and milestones are updated and formally submitted to FedRAMP within 30 days of approved modification.

There are however, changes that are considered to be routine. These changes can be standard maintenance, addition or deletion of users, the application of standard security patches, or other routine activities. While these changes individually may not have much effect on the overall security posture of the system, in aggregate they can create a formidable security issue. To combat this possibility, these routine changes should be documented as part of the CSP's standard change management process and accounted for via the CSP's internal continuous monitoring plan. Accordingly, these changes must be documented, at a minimum, within the current SSP of the system within 30 days of implementation.

Configuration Change Control Process (CCP)

Throughout the System Development Life Cycle (SDLC) system owners must be cognizant of changes to the system. Since systems routinely experience changes over time to accommodate new requirements, new technologies or new risks, they must be routinely analyzed in respect to the security posture. Minor changes typically have little impact to the security posture of a system. These changes can be standard maintenance, adding or deleting users, applying standard security patches, or other routine activities. However, significant changes require an added level of attention and action. NIST defines significant change as "*A significant change is defined as a change that is likely to affect the security state of an information system*." Changes such as installing a new operating system, port modification, new hardware platforms, or changes to the security controls should automatically trigger a re-authorization of the system via the FedRAMP process.

Minor changes must be captured and documented in the SSP of the system within 30 days of implementation. This requirement should be part of the CSP's documented internal continuous monitoring plan. Once the SSP is updated, it must be submitted to FedRAMP, and a record of the change must be maintained internally.

Major or significant changes may require re-authorization via the FedRAMP process. In order to facilitate a re-authorization, it is the responsibility of both the CSP and the sponsoring agency to notify FedRAMP of the need to make such a significant change. FedRAMP will assist and coordinate with all stakeholders the necessary steps to ensure that the change is adequately documented, tested and approved.

2.7. FISMA Reporting Requirements

FISMA established the IT security reporting requirements. OMB in conjunction with DHS enforces these reporting requirements. FISMA reporting responsibilities must be clearly defined.

FedRAMP will coordinate with CSP's and agencies to gather data associated with the cloud service offering. Only data related to the documented system security boundary of the cloud service offering will be collected by FedRAMP and reported to OMB at the appropriate time and frequency. Agencies will maintain their reporting responsibilities for their internal systems that correspond to the inter-connection between the agency and the cloud service offering.

2.8. On-going Testing of Controls and Changes to Security Controls Process

System owners and administrators have long maintained the responsibility for patch and vulnerability management. However, it has been proven time and again that this responsibility often requires a heavy use of resources as well as a documented, repeatable process to be carried out consistently and adequately. This strain on resources and lack of processes has opened the door to many malicious entities through improper patching, significant lapse in time between patch availability and patch implementation, and other security oversights. Routine system scanning and reporting is a vital aspect of continuous monitoring and thus, maintaining a robust cyber security posture.

Vulnerability patching is critical. Proprietary operating system vendors (POSV) are constantly providing patches to mitigate vulnerabilities that are discovered. In fact, regularly scheduled monthly patches are published by many POSV to be applied to the appropriate operating system. It is also the case that POSV will, from time to time, publish security patches that should be applied on systems as soon as possible due to the serious nature of the vulnerability. Systems running in virtual environment are not exempted from patching. In fact, not only are the operating systems running in a virtual environment to be patched routinely, but often-times the virtualization software itself is exposed to vulnerabilities and thus must be patched either via a vendor based solution or other technical solution.

Open source operating systems require patch and vulnerability management as well. Due to the open nature of these operating systems there needs to be a reliable distribution point for system administrators to safely and securely obtain the required patches. These patches are available at the specific vendors' website.

Database platforms, web platforms and applications, and virtually all other software applications come with their own security issues. It is not only prudent, but also necessary to stay abreast of all of the vulnerabilities that are represented by the IT infrastructure and applications that are in use.

While vulnerability management is indeed a difficult and daunting task, there are proven tools available to assist the system owner and administrator in discovering the vulnerabilities in a timely fashion. These tools must be updated prior to being run. Updates are available at the corresponding vendors' website.

With these issues in mind FedRAMP will require CSP's to provide the following:

- Monthly vulnerability scans of all servers. Tools used to perform the scan must be provided as well as the version number reflecting the latest update. A formal report of all vulnerabilities discovered, mitigated or the mitigating strategy. This report should list the vulnerabilities by severity and name. Specificity is crucial to addressing the security posture of the system. All "High" level vulnerabilities must be mitigated within thirty

days (30) days of discovery. "Moderate" level vulnerabilities must be mitigated within ninety (90) days of discovery. It is accepted that, at certain times, the application of certain security patches can cause negative effects on systems. In these situations, it is understood that compensating controls (workarounds) must be used to minimize system performance degradation while serving to mitigate the vulnerability. These "Workarounds" must be submitted to FedRAMP & the Sponsoring agency for acceptance. All reporting must reflect these activities.

- Quarterly FDCC and/or system configuration compliance scans, with a Security Content Automation Protocol (SCAP) validated tool, across the entire boundary, which verifies that all servers maintain compliance with the mandated FDCC and/or approved system configuration security settings.
- Weekly scans for malicious code. Internal scans must be performed with the appropriate updated toolset. Monthly reporting is required to be submitted to FedRAMP, where activity is summarized.
- All software operating systems and applications are required to be scanned by an appropriate tool to perform a thorough code review to discover malicious code. Mandatory reporting to FedRAMP must include tool used, tool configuration settings, scanning parameters, application scanned (name and version) and the name of the third party performing the scan. Initial report should be included with the SSP as part of the initial authorization package.
- Performance of the annual Self Assessment in accordance with NIST guidelines. CSP must perform a self-assessment annually or whenever a significant change occurs. This is necessary if there is to be a continuous awareness of the risk and security posture of the system.
- Quarterly POA&M remediation reporting. CSP must provide to FedRAMP a detailed matrix of POA&M activities using the supplied FedRAMP POA&M Template. This should include milestones met or milestones missed, resources required and validation parameters.
- Active Incident Response capabilities allow for suspect systems to be isolated and inspected for any unapproved or otherwise malicious applications.
- Quarterly boundary-wide scans are required to be performed on the defined boundary IT system inventory to validate the proper HW and SW configurations as well as search and discover rogue systems attached to the infrastructure. A summary report, inclusive of a detailed network architecture drawing must be provided to FedRAMP.
- Change Control Process meetings to determine and validate the necessity for suggested changes to HW/SW within the enterprise must be coordinated with FedRAMP to ensure that the JAB is aware of the changes being made to the system.

2.9. Incident Response

Computer security incident response has become an important component of information technology (IT) programs. Security-related threats have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventative activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the

weaknesses that were exploited, and restoring computing services. To that end, NIST SP 800-61 provides guidelines for development and initiation of an incident handling program, particularly for analyzing incident-related data and determining the appropriate response to each incident. The guidelines can be followed independently of particular hardware platforms, operating systems, protocols, or applications. As part of the authorization process the system security plan will have documented all of the "IR" or Incident Response family of controls. One of these controls (IR-8) requires the development of an Incident Response plan that will cover the life cyber of incident response as documented in the NIST SP 800-61 guidelines. The plan should outline the resources and management support that is needed to effectively maintain and mature an incident response capability. The incident response plan should include these elements:

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization
- Metrics for measuring the incident response capability
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization.

The organization's mission, strategies, and goals for incident response should help in determining the structure of its incident response capability. The incident response program structure should also be discussed within the plan. The response plan must address the possibility that incidents, including privacy breaches and classified spills, may impact the cloud and shared cloud customers. In any shared system, communication is the biggest key to success.

As part of the continuous monitoring of a system, responding to incidents will be a key element. The FedRAMP concern and its role in continuous monitoring will be to focus on how a provider conducted the incident response and any after incident actions. As represented in Figure 2: Incident response life cycle, incident response is a continually improving process.

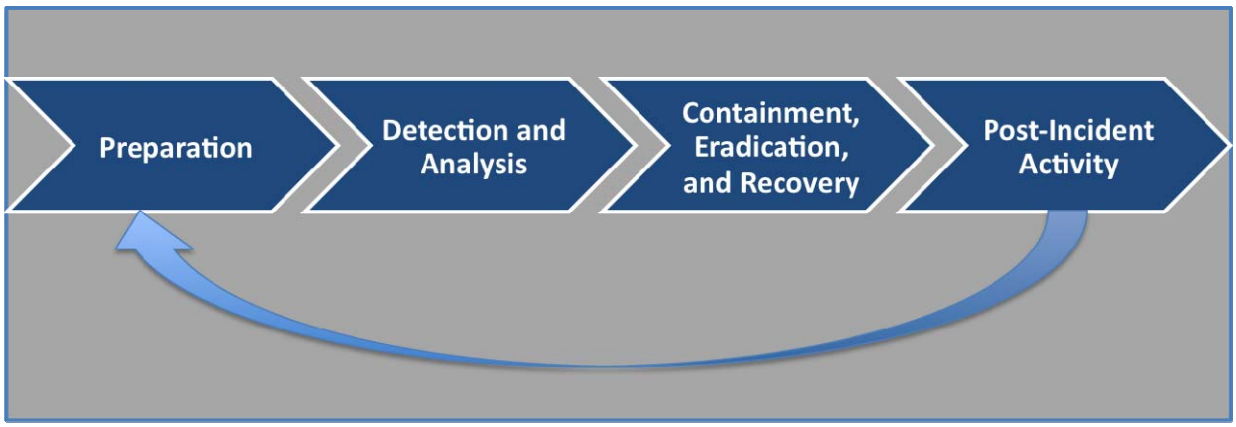

Figure 2: Incident response life cycle

One of the most important parts of incident response is also the most often omitted - learning and improving. Each incident response team should evolve to reflect new threats, improved

technology, and lessons learned. Many organizations have found that holding a "lessons learned" meeting with all involved parties after a major incident, and periodically after lesser incidents, is extremely helpful in improving security measures and the incident handling process itself. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident. Questions to be answered in the lessons learned meeting include:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently in a future occurrence?
- What corrective actions can prevent similar incidents in the future?
- What tools/resources are needed to detect, analyze, and mitigate future incidents?

Small incidents need limited post-incident analysis, with the exception of incidents performed through new attack methods that are of widespread concern and interest. After serious attacks have occurred, it is usually worthwhile to hold post-mortem meetings that cross team and organizational boundaries to provide a mechanism for information sharing. The primary consideration in holding such meetings is ensuring that the right people are involved. Not only is it important to invite people who have been involved in the incident that is being analyzed, but also wise to consider who should be invited for the purpose of facilitating future cooperation.

2.10. Independent Verification and Validation

Independent Verification and Validation (IV&V) is going to be an integral component to a successful implementation of FedRAMP. With this in mind, it must be noted that establishing and maintaining an internal expertise of FedRAMP policies, procedures and processes is going to be required. This expertise will be tasked to perform various IV&V functions with CSP's, sponsoring agencies and commercial entities obtained by CSP's with absolute independence on behalf of FedRAMP. FedRAMP IV&V will be on behalf of the JAB.

As part of these efforts, FedRAMP will periodically perform audits (both scheduled and unscheduled) related strictly to the cloud computing service offering and the established system boundary. This will include, but not be limited to:

- Scheduled annual assessments of the system security documentation;
- Verification of testing procedures;
- Validation of testing tools and assessments;
- Validation of assessment methodologies employed by the CSP and independent assessors;
- Verification of the CSP continuous monitoring program; and
- Validation of CSP risk level determination criteria.

There are several methods that must be employed to accomplish these tasks. In accordance with the new FIMSA requirement, and as a matter of implementing industry best practices, FedRAMP IV&V will be performing penetration testing. This testing will be performed with strict

adherence to the specific guidelines established by a mutually agreed upon "Rules of Engagement" agreement between FedRAMP IV&V and the target stakeholders. *Unless otherwise stated in the agreement, all penetration testing will be passive in nature to avoid unintentional consequences*. No attempts to exploit vulnerabilities will be allowed unless specified within the "Rules of Engagement" agreement.