

Continuous Monitoring White Paper

Abstract

This white paper describes an approach to the Continuous Monitoring phase of the National Institute of Standards and Technology (NIST) Certification and Accreditation (C&A) process for Federal Information Security Management Act (FISMA) compliance that blends the complementary security goals of compliance and ongoing operational security. This white paper presents a synthesis of current best practices for C&A in NIST Special Publication 800-37 and strategy for adoption of the Security Authorization Process of NIST Special Publication 800-37 Revision 1. Maintenance of information system authorization is discussed at both a strategic and tactical level and technical measures to ease support of Continuous Monitoring are enumerated.

Introduction

Continuous Monitoring is the C&A phase that achieves the complementary goals of FISMA compliance and ongoing system security. It is ultimately a means by which an organization shows due diligence in providing adequate security for the systems under its care. Continuous Monitoring is also known as the Maintenance Phase in the Security Authorization Process. This often misunderstood phase is more than the set of tasks described in NIST Special Publication 800-37; it comprises the operational security for a system throughout its lifecycle. **Figure 1** depicts how the activities in operational security overlap the process known as Continuous Monitoring. A deeper understanding of the C&A process in general and of Continuous Monitoring in particular allows organizations to better leverage security spending on compliance into effective and efficient security.

Complementary Priorities

In the Federal Government, security leaders are compelled by two ostensibly conflicting security priorities. Compliance with FISMA and other Federal security mandates drives the expenditure of money and resources on the C&A process. Simultaneously, operational security demands drive further expenditures to implement protection for critical information systems. As Continuous Monitoring is both a C&A phase and the larger portion of the ongoing operational security for systems, it stands at the intersection of these security priorities.

The vision of these as competing security priorities is unfortunate. This view leads organizations to waste money on checklist compliance without realizing the full value of the C&A process. The C&A process establishes facts about a system that are crucial to operational security, such as the information types contained, relative importance of the system to the organization, security controls that protect the system, system risks, and system boundaries. In short, the C&A process defines the “facts” necessary to practice effective and efficient operational security. In reciprocal fashion, operational security supports the C&A process. It provides the security controls to protect the system, ongoing monitoring of security controls, and ongoing identification of threats and vulnerabilities. In effect, the C&A process and ongoing operational

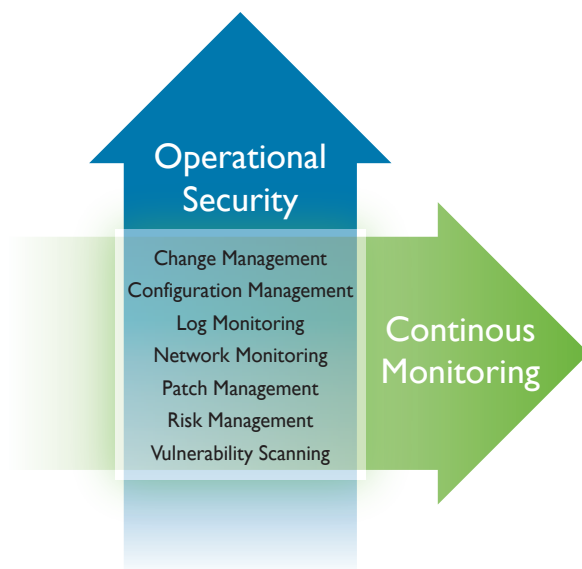


Figure 1 – The Continuous Monitoring Process overlaps with Operational Security

security priorities resolve themselves in the tasks and functions of Continuous Monitoring.

By shifting focus and recognizing the complementary nature of these security priorities, the C&A process becomes an investment in better management. To realize the full value of the C&A process it is necessary to fit its processes into the larger structures of the Risk Management Framework¹ and the System Development Life Cycle². See **Figure 2** for a visual representation of the overlap. In the Risk Management Framework (RMF), the Continuous Monitoring phase coincides with the ongoing monitoring of the security state of the organization. In the System Development Life Cycle (SDLC), the Continuous Monitoring phase is equivalent to both the Configuration Management and Control and Continuous Monitoring tasks of the Operations/Maintenance Phase as well as the System Disposition Phase. By extending the C&A process in terms of risk management, decision-makers can determine where best to expend effort and allocate resources to protect a system during the Continuous Monitoring phase.

System Documentation

Common practice in Continuous Monitoring has been to simply monitor a system with little or no security authorization documentation. The one exception were Plan of Action and Milestone (POA&M) items requiring remediation whose changes were reflected in the POA&M. This approach treated the System Security Plan (SSP) and security assessment documentation such as the Security Test and Evaluation (ST&E) as static documents updated only during the initiating phases of the C&A process; this is not a recommended best practice.

As Information System Owners and Authorizing Officials realized that the documented system knowledge gathered during the initial phases of the C&A process fell out of synch with actual system status, it was generally acknowledged that the SSP and ST&E cannot be treated as static documents. The Continuous Monitoring phase should feature the continual update of these documents to reflect the true status of the systems under management. It is only through knowledge of the actual (and current) system disposition that security can be best managed.

C&A Requirements for Continuous Monitoring

Continuous Monitoring is composed of three primary tasks: (1) Configuration Management and Control, (2) Security Control Monitoring, and (3) Status Reporting and Documentation. The primary tasks can further be broken down into nine subtasks which are described below. The goal of the Continuous Monitoring phase is to maintain the system's authorization to operate. This goal is achieved through activities which provide ongoing, near-real time risk management and operational security such as monitoring the system, ensuring the system operates in a secure fashion and reporting status to appropriate organizational personnel.

The C&A process adds to the normal practice of IT security by providing scoping guidance to more effectively manage security efforts. The initial phases of the C&A process provide three elements of primary importance to system monitoring: system baseline categorization, security controls, and known weaknesses. With these elements guiding the type and extent of monitoring, system security can most effectively be supported.

Configuration Management and Control

Configuration Management and Control consists of developing a system monitoring plan, monitoring the system for changes, and analyzing changes to determine security impact. Details of tasks involved in these activities can be found in **Figure 3**. More clearly stated, this means that an organization's security staff should be aware

C&A	SDLC	RMF
Initiation Phase	Initiation/Design	Categorize Information Systems
	Development/Acquisition	Select Security Controls
Security Certification Phase	Implementation	Implement Security Controls
Security Accreditation Phase		Assess Security Controls
Continuous Monitoring	Operation/Maintenance	Authorize Information System
	Disposal	Monitor Security Controls

Figure 2 – Phases in the Certification and Accreditation process, the System Development Life Cycle, and the Risk Management Framework overlap each other

▼ **Configuration Management and Control**

- **Security Control Monitoring Strategy** – Develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes in the information system or its environment of operation.
- **System and Environment Changes** – Document the proposed or actual changes to the information system or the environment of operation.
- **Security Impact Analysis** – Determine the security impact of the proposed or actual changes to the information system or the environment of operation in accordance with the security control monitoring strategy.

Figure 3 – Tasks involved in Configuration Management and Change Control

when changes occur and consider what those changes mean for the security of the system. The first step is to establish a security control monitoring strategy to select which security controls to monitor and how to monitor them effectively. Selection of security controls for monitoring should take into consideration the importance of the security control to both the system and the organization.

Monitoring of security controls can be done in three ways:

1. Automated processes – Vulnerability Scanners, Web Application Scanners, Patch Management software, Security Information and Event Management software and Information Security Automation Program (ISAP) / Security Content Automation Protocol (SCAP) tools
2. IT management systems – ITIL, CMMI or other change management solutions
3. Periodic audits – Auditing of sets of security controls on a regular basis.

When a new or proposed change is identified, security staff provide feedback to the Information System Owner and Authorization Officer where changes could affect the system security posture. Effort spent identifying and analyzing changes should be commensurate with the security priority of the system and the risk system changes might incur. Documentation of system changes should inform the system owner and also be reflected in SSP updates, POA&M updates, and status reports to other appropriate organization personnel.

Security Control Monitoring

Security Control Monitoring consists of the ongoing processes of security control assessment and remediation actions. Details of tasks involved in these activities can be found in **Figure 4**. The goal of this process is to ensure that the controls documented in the preliminary phases of the C&A process remain in place and operate effectively. When security controls are identified as being ineffective, either before or during the Continuous Monitoring phase, they must be remediated. The remediation method used is the periodic review of a subset of system security controls. This method is a compliance requirement which can be simplified through good documentation procedures and recognizing the best practices which achieve the goals of Security Control Monitoring.

NIST intends for security to be improved by periodic checks of the documented security controls to ensure they are in place and performing as expected. By documenting how security controls are addressed during the ST&E process, security staff can simplify subsequent security control assessments during the Continuous Monitoring phase. For example, common controls inherited from General Support Systems (GSS) or parent organizations can be quickly eliminated so that having a record of this inheritance in the Security Assessment Report (SAR) simplifies subsequent assessments. A best practice for this task is to recognize which security controls are most important to each system's function and effect on the organization. For example, selection of SC-5 Denial of Service Protection is of paramount importance to an organization's primary public web server, but can be relegated to a cursory check for an internal, minor application. By identifying the most important security controls for a specific system, these can be assessed annually to ensure the safe operation of the system. By documenting this information appropriately during the initial phases, the burden of security control assessments during Continuous Monitoring are simplified.

Status Reporting and Documentation

Status Reporting and Documentation consists of Critical Document Updates, Security Status Reporting, Ongoing Risk Determination and Acceptance, and System Removal and Decommissioning. Details of tasks involved in these activities can be found in **Figure 5**. The overall goal is to ensure that the documentation describing the security status of the system does not become stale. The POA&M is particularly important to keep current as the Office of Management and Budget (OMB) requires updates to be made available upon

▼ Security Control Monitoring

- **Ongoing Security Control Assessments** – Assess a selected subset of the security controls in the information system or the environment of operation (including those controls affected by changes to the system/environment) in accordance with the continuous monitoring strategy.
- **Ongoing Remediation Actions** – Conduct remediation actions based on the results of the selected security control assessments and outstanding items in the plan of action and milestones.

Figure 4 – Tasks involved in Security Control Monitoring

▼ Status Reporting and Documentation

- **Critical Document Updates** – Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.
- **Security Status Reporting** – Report the security status of the information system to the authorizing official and other appropriate organizational officials on a periodic basis.
- **Ongoing Risk Determination And Acceptance** – Periodically review the reported security status of the information system and determine whether the risk to organizational operations and assets, individuals, other organizations, or the Nation remains acceptable.
- **System Removal And Decommissioning** – Implement an organizationally approved information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.

Figure 5 – Tasks involved in Status Reporting and Documentation

request. However, the POA&M only reflects a single aspect of the information system, the controls known to have been inadequate. The SSP and ST&E should also be updated on an ongoing basis to support the near real-time view of the system security posture.

This task is best addressed as an extension of Configuration Management and Control. As changes occur in a system, they should be reflected in the appropriate documentation. By bundling system change, security analysis, and documentation updates, the amount of effort expended can be minimized while optimizing the benefit of this Continuous Monitoring task to ongoing system security.

When system status changes occur, they must be documented and presented to the appropriate organization officials. Significant changes may require an Authorizing Official to consider whether the risk(s) presented requires reconsideration of the operating status of the system. Additionally, these updates should be periodic and ensure all affected staff are aware of the system's status. Sometimes this is necessary due to OMB mandates but the practice is important to security beyond simply fulfilling compliance requirements.

Beyond C&A

The Continuous Monitoring phase has evolved beyond performing due diligence and satisfying FISMA compliance requirements using the C&A process. As the Risk Management Framework and the SDLC become central to system security maintenance and provide the context for monitoring a system's state, the mechanisms for Continuous Monitoring become more practical.

NIST has been working within a multi-agency initiative to produce standards and protocols for automated security maintenance. The outcome of this initiative is the Information Security Automation Program (ISAP) / Security Content Automation Protocol (SCAP) suite of interoperable security protocols and the tools which use them. The best known example of the SCAP suite is the now ubiquitous Federal Desktop Core Configuration (FDCC) initiative.

As descriptions of the tools implementing these protocols is beyond the scope of this white paper, the ISAP/SCAP suite of standards and protocols is presented below. The function of each leads logically to the type of tools which will support them as industry adoption, implementation, and product validation become widespread.

Conclusion

The often neglected Continuous Monitoring phase can be a simple and elegant means to effectively manage information systems security. Through recognizing the complementary nature of the C&A process and ongoing system security, organizations can learn to scope their security efforts efficiently. Using the tasks directed by NIST's guidance, objective periodic assessments of system security posture can be achieved while providing for ongoing FISMA compliance. Due diligence in providing for system security and FISMA compliance is becoming easier as new mechanisms are developed in support of this mission. By maintaining a current knowledge of system security state, the expense in time and resources for C&A can be considerably eased as all elements required for ongoing authorization are readily available.

¹ NIST SP 800-039 Draft 2, Managing Risk from Information Systems: An Organizational Perspective (2008-04)

² NIST SP 800-064 Revision 1, Security Considerations in the Information System Development Life Cycle (2004-06)



1515 N. Courthouse Road
Suite 310
Arlington, VA 22201
703.841.5500 tel
703.841.5501 fax

www.onpointcorp.com