NIST Special Publication 800-137

Information Security Continuous Monitoring for Federal Information Systems and Organizations

Kelley Dempsey
Arnold Johnson
Alicia Clay Jones
Angela Orebaugh
Matthew Scholl
Kevin Stine

I N F O R M A T I O N S E C U R I T Y

INITIAL PUBLIC DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

DECEMBER 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in Circular A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in Circular A-130, Appendix III.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Special Publication 800-137, 38 pages

(December 2010)

Public comment period: December 16, 2010 – March 15, 2011

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic mail: 800-137comments@nist.gov

Acknowledgements

The authors, Kelley Dempsey, Arnold Johnson, Matthew Scholl and Kevin Stine of the National Institute of Standards and Technology (NIST) and Alicia Clay Jones and Angela Orebaugh of Booz Allen Hamilton, wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. The authors would like to acknowledge their colleagues for their keen and insightful assistance with technical issues throughout the development of the document.

Table of Contents

CHAPTER ONE INTRODUCTION **1**
1.1 BACKGROUND 2
1.2 RELATIONSHIP TO OTHER GUIDANCE DOCUMENTS 2
1.3 PURPOSE 4
1.4 TARGET AUDIENCE 4
1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION 4
CHAPTER TWO THE FUNDAMENTALS **6**
2.1 ORGANIZATION-WIDE VIEW OF CONTINUOUS MONITORING 6
2.2 ONGOING SYSTEM AUTHORIZATIONS 13
2.3 ROLE OF AUTOMATION IN CONTINUOUS MONITORING 15
2.4 CONTINUOUS MONITORING ROLES AND RESPONSIBILITIES 16
CHAPTER THREE THE PROCESS **19**
3.1 DEFINE CONTINUOUS MONITORING STRATEGY 20
3.2 ESTABLISH MEASURES AND METRICS 26
3.3 ESTABLISH MONITORING AND ASSESSMENT FREQUENCIES 28
3.4 IMPLEMENT A CONTINUOUS MONITORING PROGRAM 33
3.5 ANALYZE DATA AND REPORT FINDINGS 33
3.6 RESPOND TO FINDINGS 35
3.7 REVIEW AND UPDATE THE MONITORING PROGRAM AND STRATEGY 36

APPENDIX A REFERENCES A-1

APPENDIX B GLOSSARY B-1

APPENDIX C ACRONYMS C-1

APPENDIX D TECHNOLOGIES FOR ENABLING CONTINUOUS MONITORING D-1

EXECUTIVE SUMMARY

In today's environment where many, if not all, of an organization's mission critical functions are dependent upon information technology, the ability to manage this technology and to assure confidentiality, integrity and availability of information is now also mission critical. In designing the enterprise architecture and corresponding security architecture, an organization seek to securely meet the IT infrastructure needs of its governance structure, missions, and core business processes. Information security is a dynamic process that must be effectively managed to respond to new vulnerabilities, evolving threats, and an organization's constantly changing enterprise architecture and operational environment.

The Risk Management Framework (RMF)[1], developed by NIST, describes a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The RMF consists of six steps. Ongoing monitoring (i.e., Step 6 in the RMF that follows the initial assessment and authorization steps) is a critical part of that risk management process. In addition, an organization's overall security architecture and accompanying security program are monitored to ensure that organization-wide operations remain within an acceptable level of risk, despite the changes that occur. Should operations fall outside of the stated levels of risk tolerance, relevant and accurate information is needed to make risk management decisions. Timely information is vital, particularly when resources are limited and agencies must prioritize their efforts.

> Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The objective is to conduct ongoing monitoring of the security of an organization's networks, information, and systems, and respond by accepting, avoiding/rejecting, transferring/sharing, or mitigating risk as situations change.

Any effort or process, intended to support ongoing monitoring of information security across an organization, must begin with defining a comprehensive continuous monitoring strategy spanning technology, processes, procedures, operating environments, and people. This strategy:

- Is grounded in a clear expression of organizational risk tolerance;
- Includes measures and metrics that provide meaningful indications of security status at all organizational tiers;
- Ensures continued effectiveness of all security controls;
- Is informed by and helps to maintain visibility into all organizational IT assets;
- Ensures knowledge and control of changes through inventory and configuration management;
- Proactively manages the security impact of changes;
- Maintains awareness of threats and vulnerabilities; and
- Helps officials set priorities and manage risk within organizational risk tolerance levels.

[1] SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems.*

A continuous monitoring program is established to collect information in accordance with pre-established metrics, utilizing information readily available in part through implemented security controls. Tools, technologies and methodologies including sampling, common protocols, and reference architectures make organization-wide manual and automated data collection, aggregation, analysis, and reporting practical. Organizational officials collect and analyze the data regularly and as often as needed to manage risk as appropriate for each organizational tier. This involves the entire organization, from senior leaders providing governance and strategic vision to individuals developing, implementing, and operating individual systems in support of the organization's core missions and business processes. Subsequently, determinations are made from an organizational perspective on whether to conduct mitigation activities, or reject, transfer, or accept risk.

Organizations' security architectures, operational security capabilities, and monitoring processes will improve and mature over time to better respond to the dynamic threat and vulnerability landscape. The continuous monitoring strategy and program are routinely reviewed for relevancy and are revised as needed to increase visibility into assets and awareness of vulnerabilities, further enable data driven control of the security of an organization's information infrastructure, and increase organizational resiliency.

Organization-wide monitoring cannot be efficiently achieved through manual processes alone or through automated processes alone; however, automation, including the use of automated support tools (e.g., vulnerability scanning tools, network scanning devices), can make the process of continuous monitoring more cost-effective, consistent, and efficient. Many of the technical security controls defined in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, are good candidates for monitoring using automated tools and techniques. Real-time monitoring of implemented technical controls using automated tools can provide an organization with a much more dynamic view of the security state of those controls. It is also important to recognize that with any comprehensive information security program, all implemented security controls, including management and operational controls, must be regularly assessed for effectiveness, even if the monitoring of such controls cannot be automated or is not easily automated.

Organizations take the following steps to establish, implement, and maintain a continuous monitoring program. The process consists of the following steps:

- Define continuous monitoring strategy;
- Establish measures and metrics;
- Establish monitoring and assessment frequencies;
- Implement continuous monitoring program;
- Analyze data and report findings;
- Respond with mitigating strategies, or reject, transfer or accept risk; and
- Review and update continuous monitoring strategy and program.

Though this process is not identical to the tasks listed in Step 6, Monitor, of the Risk Management Framework, there is overlap between the organization-wide and system-level

processes and, where practical, one process supports the other. Configuration management and security impact analysis are vital components of sound information security management practices, and are part of an organization's continuous monitoring program. The use of security automation and technologies currently available to support continuous monitoring are considered (e.g., IDPS, vulnerability assessment, and configuration management tools).

CHAPTER ONE

INTRODUCTION

Continuous monitoring is defined as maintaining ongoing awareness to support organizational risk decisions. More specifically, *information security* continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. This publication specifically addresses information security continuous monitoring including assessment and analysis of security control effectiveness and of organizational security status in accordance with organizational risk tolerance.[2] Security control effectiveness is measured by correctness of implementation and by how adequately the implemented controls meet organizational needs in accordance with current risk tolerance (i.e. is the control implemented in accordance with the security plan and is the security plan adequate). Organizational security status is determined using measures and metrics established by the organization to best convey the standing of an organization's information and information systems along with organizational resiliency given known threat information. This necessitates maintaining situational awareness of all systems and system configurations across the organization, maintaining an understanding of threats and threat activities, evaluating the security impact of actual and proposed changes, assessing all security controls, collecting, correlating and analyzing security-related information, providing actionable communication of security status across all levels of the organization, and active management of risk by organizational officials. Information security continuous monitoring is a critical part of organization-wide risk management.[3] This guidance document builds on the concepts introduced in NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Appendix G. The objective of an organization-wide information security continuous monitoring program is to ensure that deployed security controls continue to be effective over time, in light of the inevitable changes that occur and that operations remain within stated organizational risk tolerances. In cases where security controls are determined to be inadequate, continuous monitoring programs facilitate prioritized security response actions based on risk.

Continuous monitoring gives organizational officials access to security-related information in near real-time, enabling timely risk-management decisions, including authorization decisions. The frequency at which information is collected varies with the specific measurement under consideration and depends in part upon the ability of the organization to collect the data and to act on it. Near real-time awareness of some security-related information is obtained through tools designed for automated data collection and reporting. While this document encourages the use of automation, it is recognized that many aspects of continuous monitoring programs are not easily automated.

An information security continuous monitoring strategy is only meaningful within the context of broader organizational needs, objectives or strategies, and as a part of a broader risk management strategy enabling timely management, assessment, and response to emerging security issues. Information collected from continuous monitoring programs can support ongoing authorization

[2] The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions as needed to adequately protect organization information. Data collection, no matter how frequent, is still collected at discrete intervals.

[3] See NIST SP 800-39 DRAFT, *Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View, December 2010.*

decisions. Continuous monitoring supports, but does not supplant, the need for system reauthorization.

Continuous monitoring is most effective when automated mechanisms are employed where possible. It can support frequent automated updates to security plans, security assessment reports, plans of action and milestones, hardware and software inventories and other system information. As such, a well designed strategy for continuous monitoring supports information system re-authorizations, administrative processes such as external reporting requirements, inventories of systems, hardware, software and connections, as well as operational processes such as incident response, configuration management and control, identity and access management, and strategies for addressing threats, including advanced persistent threats.

1.1 BACKGROUND

The concept of monitoring information system security has long been recognized as sound management practice. In 1997, Office of Management and Budget (OMB) Circular A-130, Appendix III[4] required agencies to *review* their information systems' security controls and ensure that system changes do not have a significant impact on security, that security plans remain effective, and that security controls continue to perform as intended.

The Federal Information Security Management Act (FISMA) of 2002 further emphasized the importance of continuously monitoring information system security by requiring agencies to conduct assessments of security controls at a frequency depending on risk, but no less than annually.

Continuous monitoring is a critical step in an organization's Risk Management Framework (RMF). In NIST SP 800-37, the concept is expanded to include an organization-wide perspective, integration with the system development life cycle (SDLC), and support for ongoing authorizations.

Most recently, OMB issued memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.[5] The memorandum provides instructions for annual FISMA reporting, and requires agencies to continuously monitor security-related information from across the enterprise in a manageable and actionable way

Tools supporting automated monitoring of some aspects of information systems have become an effective means for both data capture and data analysis. Ease of use, accessibility, and broad applicability across products and across vendors mean that monitoring tools can be readily deployed in support of near real-time risk based decision making.

1.2 RELATIONSHIP TO OTHER GUIDANCE DOCUMENTS

NIST SP 800-37 identifies the following as elements essential to a successful organization-wide continuous monitoring program:

[4] OMB Circular A-130 is available at http://www.whitehouse.gov/omb/circulars_a130_a130trans4.

[5] OMB memorandum M-10-15 is available at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf

- Configuration management and change control;
- Security impact analyses;
- (Ongoing) assessment of system security controls;
- Security status monitoring and reporting;
- Active involvement of organizational officials in the ongoing management of information system security-related risks.

Similarly, NIST SP 800-37 attributes the following tasks to the monitoring step (Step 6) in the RMF for operational information systems:

- Determine the security impact of proposed or actual changes;
- Assess a system's technical, management, and operational security controls in accordance with the organization-defined monitoring strategy frequency as approved by system officials to maintain a continuous authorization to operate;
- Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones;
- Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process;
- Report the security status of the information system to appropriate organizational officials on an ongoing basis;
- Review the reported security status to determine whether the risk remains acceptable; and
- Implement an information system decommissioning strategy, when needed.

A similar process is also reflected in NIST SP 800-39 and is evident in the continuous monitoring process. NIST SP 800-39 complements the guidance provided in this document, including discussions of risk tolerance.

The organizational tiers (i.e., levels, as discussed in Chapter 2) herein mirror those described in NIST SP 800-37 and NIST SP 800-39 where Tier 1 is organization; Tier 2 is mission/business; and Tier 3 is information system. In NIST SP 800-37, these tiers are used to address risk management from varying organizational perspectives. In this document, the tiers are used to address perspectives for continuous monitoring for each tier. Organization-wide, tier-specific policies, procedures, and continuous monitoring responsibilities are included for the organization, mission/business, and information system tiers. Automation is leveraged where possible, and manual (i.e., procedural) monitoring methodologies are implemented where automation is not practical or possible.

The continuous monitoring program will evolve over time as the program matures in general, additional tools and resources become available, measurement and automation capabilities mature, and changes are implemented to ensure continuous improvement in the organizational security posture and in the organization's security program. The monitoring strategy is regularly reviewed for relevancy and accuracy in reflecting organizational risk tolerances, correctness of

measurements, applicability of metrics, and effectiveness in supporting risk management decisions.

1.3 PURPOSE

The purpose of this guideline is to assist organizations in the development of a continuous monitoring strategy and the implementation of a continuous monitoring program providing visibility into organizational assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls. It provides ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance *as well as* the information needed to respond to risk in a timely manner should observations indicate that the security controls are inadequate.

1.4 TARGET AUDIENCE

This publication serves individuals associated with the design, development, implementation, operation, maintenance, and disposition of federal information systems including:

- Individuals with mission/business ownership responsibilities or fiduciary responsibilities (e.g., heads of federal agencies, chief executive officers, chief financial officers);
- Individuals with information system development and integration responsibilities (e.g., program managers, information technology product developers, information system developers, information systems integrators, enterprise architects, information security architects);
- Individuals with information system and/or security management/oversight responsibilities (e.g., senior leaders, risk executives, authorizing officials, chief information officers, senior information security officers[6]);
- Individuals with information system and security control assessment and monitoring responsibilities (e.g., system evaluators, assessors/assessment teams, independent verification and validation assessors, auditors, or information system owners); and
- Individuals with information security implementation and operational responsibilities (e.g., information system owners, common control providers, information owners/stewards, mission/business owners, information security architects, information system security engineers/officers).

1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- Chapter Two describes the fundamentals of ongoing management of information security in support of risk management.
- Chapter Three describes the process of continuous monitoring, including implementation guidance.

[6] At the *agency* level, this position is known as the Senior Agency Information Security Officer. Organizations may also refer to this position as the Chief Information Security Officer.

- Supporting appendices provide additional information regarding information security continuous monitoring including: (i) general references; (ii) definitions and terms; (iii) acronyms; and (iv) descriptions of automated technologies to facilitate information security continuous monitoring.

CHAPTER TWO

THE FUNDAMENTALS

ONGOING MONITORING IN SUPPORT OF RISK MANAGEMENT

Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. This chapter describes the fundamental concepts associated with organization-wide continuous monitoring of information security and the application of continuous monitoring in support of ongoing system authorization. Continuous monitoring is often wrongly thought of solely in terms of periodic security control assessment and system reauthorization *or* security status monitoring, analysis, and reporting. In order to effectively address ever increasing security challenges, a well-designed continuous monitoring strategy for information security addresses both and incorporates processes to respond to findings with response actions as necessary. Continuous monitoring helps ensure ongoing situational awareness and control of the security of systems across the organization and ongoing knowledge of associated threats and vulnerabilities, despite inevitable changes to organizational information systems and their environments of operation. Examples of organizational monitoring needs include system component inventories, a near real time understanding of threat activity and threat actions to organizational systems and infrastructures and how this activity can exploit existing vulnerabilities, configuration management, security impact analysis requirements for changes, status reporting, leadership review of information security requirements at all organizational levels, security control assessments, and ongoing system authorizations.

In organization-wide continuous monitoring, the strategy is driven by governance level risk management goals and objectives, while its implementation occurs at all organizational levels with data collection primarily occurring at the system level. The information provided by continuous monitoring helps officials manage information system risk in near real-time. This includes aggregated risk from many individual information systems, for the organization as a whole, or for a specific information system. Through the use of automation, it is possible to monitor a greater number of security measures and metrics with fewer resources, higher frequencies, larger sample sizes[7], and with greater consistency and reliability than is feasible using manual processes.[8] Organizations regularly review the continuous monitoring strategy to ensure that metrics continue to be relevant, meaningful, and supportive of risk management decisions made by organizational officials at all organizational levels.

2.1 ORGANIZATION-WIDE VIEW OF CONTINUOUS MONITORING

Maintaining an up-to-date view of information security and risks across an organization is a complex, multifaceted undertaking. It requires the involvement of the entire organization, from senior leaders providing governance and strategic vision at Tier 1 to individuals developing, implementing, and operating individual systems in support of the organization's core missions

[7] If an organization does not have the resources or infrastructure necessary to assess every relevant object within its information infrastructure, sampling is an approach that may be useful in reducing the level of effort associated with continuous monitoring. Additional information is provided in section 3.1.3.

[8] A "measure" is the result of gathering data from sources you know and have. A "metric" is designed to organize data into meaningful information to support decision making.

and business processes. Figure 2-1 illustrates a tiered approach to organization-wide information security continuous monitoring in support of risk management. Risk tolerance decisions made by the risk executive (function)[9] drive Tier 1 continuous monitoring policy, Tier 2 procedures, and Tier 3 implementation activities. Procedures, metrics, and templates at the mission/business level facilitate continuous monitoring at the mission/business and system levels. Likewise, the ongoing monitoring activities implemented at the system level provide near real-time system-level security-related information to the Authorizing Official (AO) in support of ongoing system authorization and to the risk executive (function) in support of ongoing organizational risk management. An organization's continuous monitoring strategy incorporates information such as the security risk tolerance, performance metrics, data types and procedures, specifications, techniques and tools for gathering appropriate data – and plans for acting on the information obtained.[10] Security-related information is taken from system-specific, common, and hybrid security controls, including the program management (PM) security controls. Metrics are designed to acquire data in a form appropriate for use by officials at all levels of the organization. Data collection, analysis and reporting are automated where possible.[11]

[9] See glossary

[10] See Chapter 3 for a complete discussion of continuous monitoring implementation strategy.

[11] Care must be taken in determining how best to use security-related information (measures and data feeds) from individual information systems in calculating organizational metrics for security and risk. Dashboards and metrics, designed to provide organizational situational awareness of security and risk, can provide a false sense of security if used without continued assurance of the relevance of the metrics and of the measures underlying those metrics.

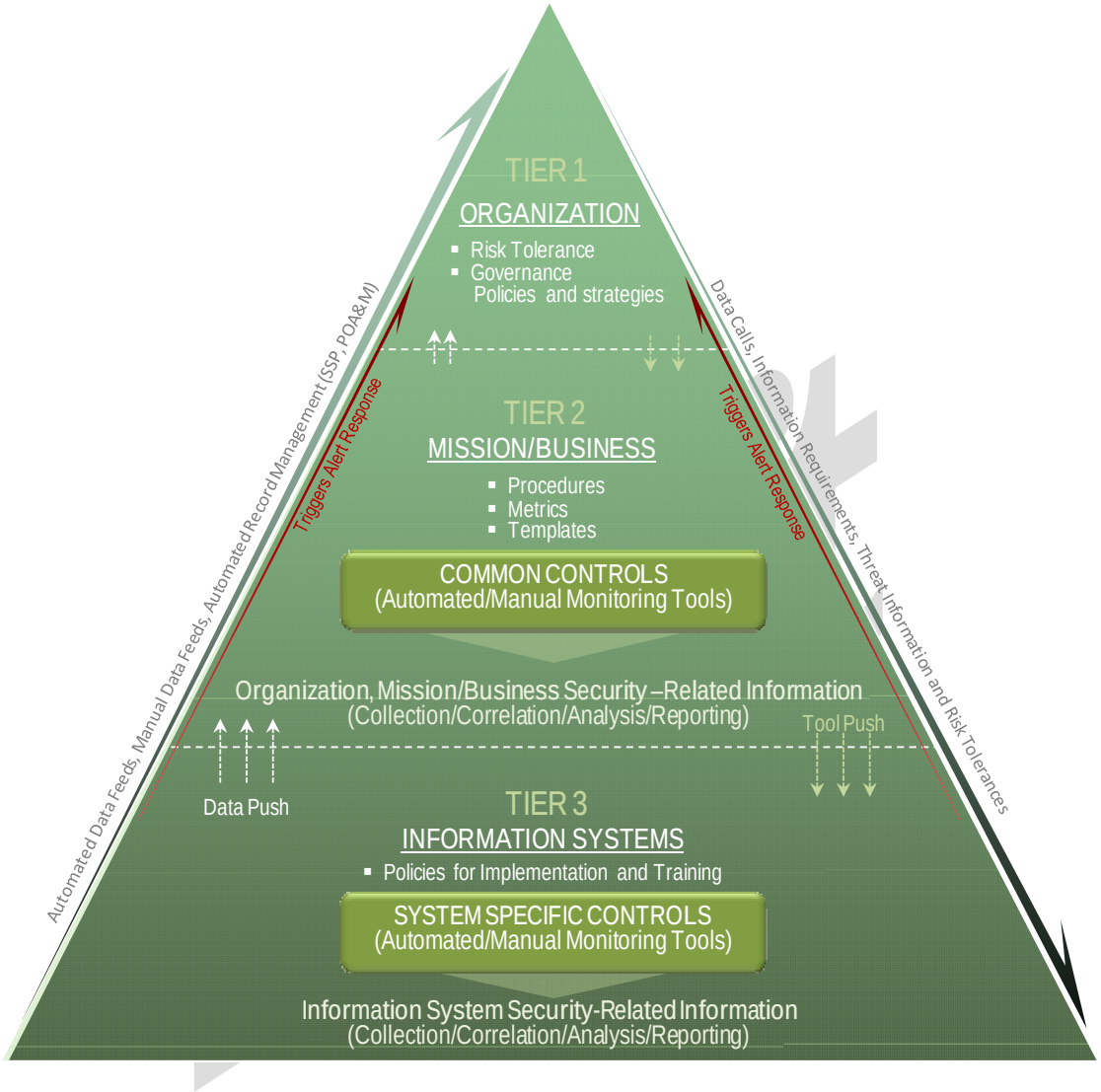

Figure 2-1. Organization-wide Continuous Monitoring

An organization-wide approach to continuous monitoring of information and information system security supports risk-related decision making at the *organization/governance* level (Tier 1), the *mission/business process* level (Tier 2), and the *information systems* level (Tier 3).[12]

Organization/Governance level (Tier 1). Tier 1 risk management activities address high level information security governance policy and overall risk to the organization, its missions and its core business processes. At this level, the strategic criteria for continuous monitoring of information security are defined by the organization's risk tolerance, how the organization plans to monitor risk given the inevitable changes to organizational information systems and their environments of operation, and the degree and type of oversight the organization plans to use to ensure that the risk management strategy is being effectively carried out. Metrics defined and monitored by officials at this level are designed to deliver information necessary to make risk

[12] NIST Special Publication 800-39 provides guidance on the holistic approach to risk management.

management decisions in support of the organization's governance structure. These metrics are calculated in part based on measures from common and program management controls, as well as on measures from information system security controls. The metrics and the frequency with which they are monitored[13] and reported are determined by requirements to maintain operations within organizational risk tolerances. As part of the overall governance structure established by the organization, the Tier 1 risk management strategy and associated monitoring requirements are propagated down throughout Tiers 2 and 3.

Mission/Business level (Tier 2). Officials accountable for one or more organizational missions or core business processes oversee risk management activities in terms of a given core business process and in accordance with stated mission priorities. The Tier 2 strategic criteria for continuous monitoring of information security are defined by how mission and core business processes are prioritized with respect to the overall goals and objectives of the organization, the types of information needed to execute successfully the stated missions and business processes, and the organization wide information security program strategy. Metrics and the frequency with which they are monitored and reported are determined in part by the objectives and priorities of the mission or business process, and measurement capabilities inherent in the infrastructure.[14] Security-related information may come from common, hybrid, and system level controls. Common controls are selected and allocated at Tier 1 but are typically implemented and managed at Tier 2 and are used to serve multiple information systems, missions, and business processes. There are many benefits of using common controls including consistency of implementation, cost efficiencies, and built-in assessor independence for organizations leveraging common control security-related information for ongoing information system authorization or for re-authorization. The Program Management (PM) controls are a special type of common controls that are implemented at Tier 2. The PM controls are uniquely important to a continuous monitoring strategy. The associated metrics provide insight into the ongoing effectiveness of the security program, thus supporting risk management decisions. Consequently, Tier 1 has a role in determining these controls. Organizations monitor, assess, evaluate, and respond to risk with varying degrees of autonomy below Tier 2. Diverse risk assessment methods may be used across an organization. Metrics and dashboards can be useful at Tier 2 in assessing, normalizing, and correlating monitoring activities below the mission/business level in a meaningful manner.

Information Systems level (Tier 3). Continuous monitoring activities at Tier 3 address risk management from an *information system* perspective. The continuous monitoring requirements include ensuring that all system security controls (technical, operational *and* management controls) are implemented correctly, operate as intended, produce the desired outcome with respect to meeting the security requirements for the system as planned, and continue to secure the system effectively. Often security alerts, security incidents, and identified threat activities are generated at this level. The continuous monitoring strategy for the information system also ensures that security-related information supports the monitoring requirements of other organizational tiers as well. Data feeds from system specific and hybrid controls, along with associated security status reporting, support risk-based decisions at the organization and mission/business levels. Since the information is tailored for each level and delivered in ways that inform risk management security decision making at all levels. Those resulting decisions impact the continuous monitoring strategy applied at the information system level.[15] Measures

[13] Monitoring organizationally defined metrics is referred to as security status monitoring throughout this document.

[14] As an organization's technical and human capitol capabilities mature, monitoring capabilities increase.

[15] A continuous monitoring strategy for an individual system may also include measures and metrics related to its

from continuous monitoring originating at the system level can be used to support metrics and manage risk across organizational, missions and business processes. A continuous monitoring program design is intended to support vital organizational requirements for real-time or near real-time security-related information. Ongoing authorization is of particular concern and is discussed in section 2.3.

The following processes are introduced in NIST SP 800-37 as essential to organization-wide continuous monitoring:

- Ongoing **assessment of security controls** (including system-specific, hybrid, common controls and PM controls) with assessment frequencies based on an organization-wide continuous monitoring strategy and individual system authorization strategies;
- **Configuration management and change control** processes for organizational information systems, throughout their SDLCs, and with consideration of their operating environments and their role(s) in supporting the organization's missions and core business processes;
- **Security impact analyses** (SIA) on changes to organizational information systems and their environments of operation for any adverse security impact to systems, mission/business and/or organizational functions which said systems support. Considerations include the impact to the enterprise architecture due to the commissioning or decommissioning of systems.
- **Security status reporting** to organizational officials designed to enable data-driven risk mitigation decisions with minimal response times and acceptable data latencies[16]. Considerations include organization relevant threat data where available.[17]
- **Active involvement of organizational officials** in continuous monitoring and the ongoing management of information security-related risks.

Figure 2-2 illustrates how these five elements work together to achieve effective continuous monitoring.

Ongoing control of information security risk requires security control assessment, security status monitoring, security status analysis, and security status reporting. The resulting information is used in an organization-wide continuous monitoring strategy, in order to maintain visibility into assets and awareness of vulnerabilities and threats and to ensure that implemented security controls continue to be effective. Configuration management and change control processes help to maintain a secure baseline configuration. Security control assessments help ensure that security controls are implemented correctly, operating as intended, and meeting stated security objectives. Security status monitoring ensures that organizational officials have the metrics-based information necessary to make risk management decisions. SIA processes, used with

potential impact on other systems.

[16] Data latency is a measure of the currency of data (in this case, security-related information). It refers to the time between when the information was collected and when it is used.

[17] Knowledge of data latencies is related to the effectiveness of an organizational response to threats and incidents and will impact how an organization responds using an appropriate risk decision. Understanding of data latencies allow an organization to respond "where the threat and/or vulnerability is and where it is headed" in an organization rather than where it was. This is an important data point for organizations to use in shortening a risk decision cycle when responding to threats and/or vulnerabilities.

configuration management and change control as well as ongoing assessments, help maintain visibility into assets, awareness of vulnerabilities including evolving threats and assurance that implemented and planned security controls continue to be effective as changes occur to information systems and their operating environments. Active involvement of management in reviewing and responding to security status reports helps ensure awareness of vulnerabilities throughout the organization, provides insight into the ability of implemented controls to mitigate those vulnerabilities, helps ensure availability of timely, actionable information, and promotes ongoing control of operations to within organizational risk tolerances.

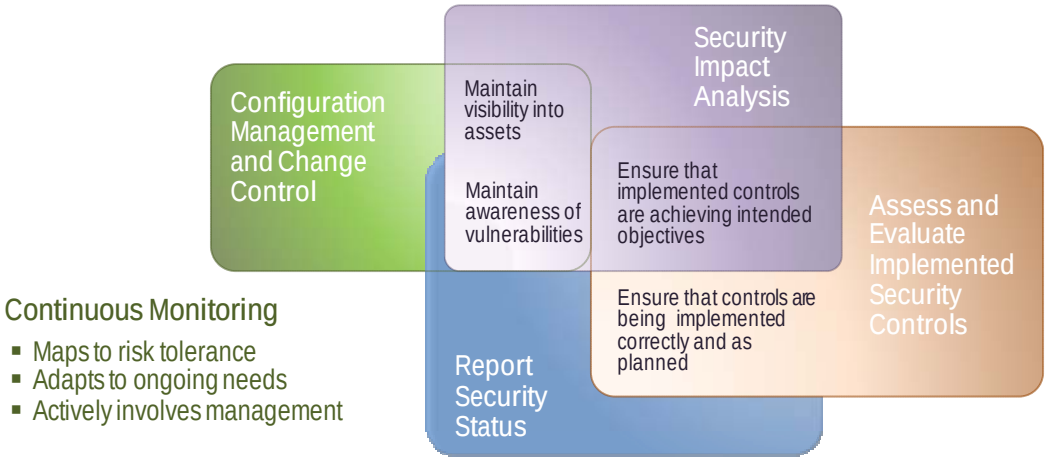

Figure 2- 2. Elements of an Effective Continuous Monitoring Program

The key concepts stated above are not unique to continuous monitoring processes. These concepts have long been accepted as sound information system security management practices. Detailed guidance already exists on some of these topics as they apply to information systems. Security control assessments are discussed in NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*. Configuration management and security impact analysis are addressed in NIST SP 800-128 DRAFT *Guide for Security Configuration Management of Information Systems*. Measures and metrics for security status monitoring and reporting are discussed in NIST SP 800-55, *Performance Measurement Guide for Information Security*. The roles and responsibilities of management in a continuous monitoring program are described below in section 2.5. Additional perspective on organization-wide configuration management and control processes, security impact analysis, and security status reporting is provided in this guideline.

2.1.1 DEVELOP CONFIGURATION MANAGEMENT AND CONTROL PROCESSES

The configuration of an information system and its components has a direct impact on the system's ability to protect the confidentiality, integrity, and availability of information stored, processed, or transmitted. While changes to the configuration of an information system are often necessary to accommodate changing business functions and information security needs, these changes can adversely impact the previously established security posture. Changes may also occur unintentionally (or through malicious actions) in the natural course of operations. Changes also occur at the level of the enterprise architecture and include addition or removal of information systems or changes to information or information system requirements associated

with mission and business processes. Configuration management and control processes are an important precondition to the success of an organization's information security continuous monitoring program. Without knowledge and control of changes to the enterprise architecture, down to the information system component level, monitoring will result in inaccurate risk data.

Configuration management and control processes are implemented at the system level (or pushed down from the mission/business level), while the policies governing these processes are typically established at the organizational and mission/business levels.

Automation in continuous monitoring programs can have a significant impact on system level configuration management processes. Tools and technologies that can automatically assess information system components within the information environment can provide considerable efficiency and accuracy in managing the myriad information system configurations over manual approaches. An automated tool can scan information system components (e.g., Web server, database server, network devices), identify the current configuration settings, and indicate where they are noncompliant with policy. Such tools may also be able to import settings from one or more secure configuration specifications such as those provided through the Security Content Automation Protocol (SCAP)[18] and then allow for tailoring the settings to the organization's information environment.[19]

Detailed information on developing and implementing a configuration management and control process for an information system is provided in NIST SP 800-128 DRAFT.

2.1.2 DEVELOP SECURITY IMPACT ANALYSIS PROCESS AND CONDUCT ANALYSES

Security impact analysis (SIA) at the system level determines the extent to which changes to the information system or its environment of operation affect the security state of the system. Changes to the information system or its environment of operation may affect the security controls currently in place (including system-specific, hybrid, and common controls), produce new vulnerabilities in the system, or generate requirements for new security controls that were not needed previously. SIAs also apply to commissioning and decommissioning of systems within the enterprise architecture. An effective security impact analysis process is an essential factor in the organization's configuration management process and thus also to the organization's continuous monitoring program.

Detailed information on developing and implementing a security impact analysis process and conducting security impact analyses is provided in NIST SP 800-128 DRAFT.

2.1.3 SECURITY STATUS REPORTING

Organizational officials at all levels require appropriate, accurate, and up-to-date security-related information to support ongoing management of information security risks. Security status reports include data on assessments of specific controls as well as metrics to convey security status in terms relevant to officials at different organizational tiers.[20] In the case of the latter, data is normalized so that information from various assessors and/or information from various systems

[18] See http://nvd.nist.gov for more information on SCAP.

[19] One such example is Federal Desktop Core Configuration (FDCC) settings. See OMB Memorandum M-08-22 at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-22.pdf.

[20] See NIST SP 800-55 for more information on metrics.

can be combined, correlated, analyzed, and put into appropriate context for organizational officials' decision making at every tier, including authorization decisions.

Considerations of threats and threat activity are a critical data input for security status reporting. Incidents, suspected threat activity, updated threat models, results of red-team activity, shared threat reporting from outside the organization and automated threat data assist in providing risk management information at all levels. Clear understanding and communication of threat information and organizational risk tolerances, traced to measures and metrics can be used to automate alerting and initial responses when threats are identified that have potential to exploit vulnerabilities and pose risk to assets. An information security continuous monitoring program can give an organization the ability to monitor emerging threat patterns and reconcile the data against known system assets and vulnerabilities to determine if a specific attack is developed which exploits a vulnerability of an implemented technology.

2.2 ONGOING SYSTEM AUTHORIZATIONS

Security-related information collected through continuous monitoring programs can support ongoing authorization or reauthorization decisions. The process for obtaining system authorizations, and more generally for managing information security and information *system-related* organizational risk, is the RMF. The RMF, illustrated in Figure 2-2, provides a disciplined and structured process that integrates information system security and risk management activities into the SDLC. The monitoring step (Step 6) of the RMF includes interactions between the three tiers as illustrated in the organizational view of continuous monitoring in Figure 2-1. These interactions between the system level and the higher organizational tiers include feedback from System Owner and Authorizing Official on system security control assessments and authorization to the risk executive (function) at Tier 1.[21] There is also dissemination of updated risk-related information such as vulnerability and threat data and organizational risk tolerance from Tiers 1 and 2 to authorizing officials and information system owners. When the RMF is applied within an organization that has also implemented a robust continuous monitoring strategy, organizational officials are provided with a near real-time view of the organizational security posture and each system's contribution to said posture.

[21] NIST Special Publication 800-37 describes the interaction of the risk executive (function) in the context of the RMF.

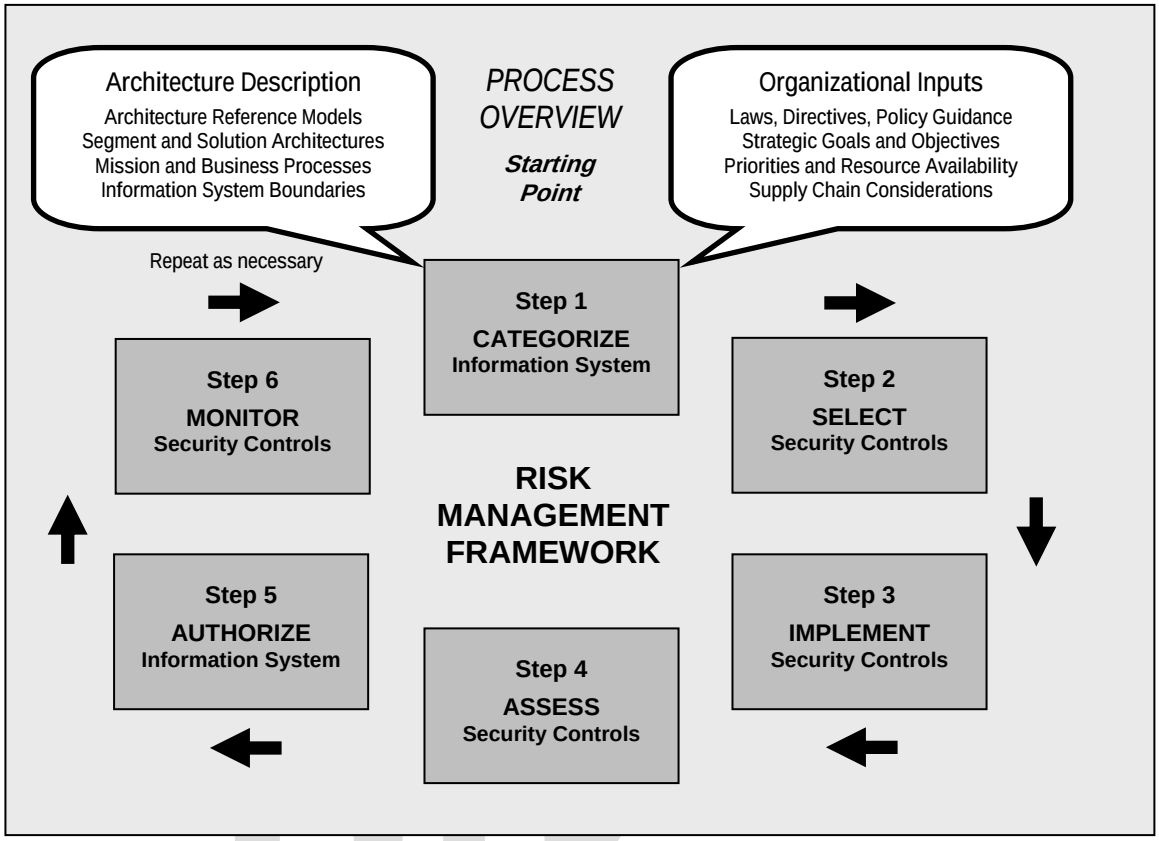

Figure 2- 3. Risk Management Framework

The output of a strategically designed and well-managed organization-wide continuous monitoring program can be used to maintain a system's authorization to operate and keep required system information and data (i.e., System Security Plan together with Risk Assessment Report, Security Assessment Report, and POA&M) up-to-date on an ongoing basis. Security management and reporting tools may provide functionality to automate updates to key evidence needed for on-demand authorization decisions. Initial authorization to operate is based on evidence available at one point in time, but systems and environments of operation change. Ongoing assessment of security control effectiveness supports a system's security authorization over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Through continuous monitoring, new threat or vulnerability information is evaluated as it becomes available, permitting organizations to make adjustments to security requirements or individual controls as needed to maintain authorization decisions in near real-time. Continuous monitoring drives organizations towards risk-based rather than compliance-based decisions regarding the ongoing authorization to operate information systems by providing evolving threat activity or vulnerability information in near real-time. A security control assessment and risk determination process, otherwise static between authorizations, is thus transformed into a dynamic process that supports timely risk mitigation actions and cost effective, ongoing authorizations. Continuous monitoring of threats, vulnerabilities and security control effectiveness provides situational awareness for risk-based support of ongoing system authorization decisions. An appropriately designed continuous

monitoring strategy and program supports continuous authorization of type authorizations, as well as single, joint and leveraged authorizations.[22]

Continuous monitoring in support of ongoing assessment and authorization has the potential to be resource intensive and time consuming. It is impractical to collect security-related information and assess every aspect of every security control deployed across an organization at all times. A more practical approach is to establish reasonable assessment frequencies for collecting of security-related information. The frequency of assessments should be sufficient to assure adequate security commensurate with risk, as determined by system categorization and continuous monitoring strategy requirements. Sampling of information system security objects, rather than 100% inspection, can also be an efficient and effective means of monitoring, particularly in cases where monitoring is not automated. Important considerations in determining sample sizes and monitoring frequencies are discussed in Chapter 3.

Monitoring frequencies (e.g., annually, quarterly, monthly, daily) are not static, and they are not identical across all metrics. Security control assessment and monitoring frequencies, for example, are adjusted to support changes in organizational information systems or their environments of operation, including emerging information on security threats and vulnerabilities. The priorities for continuous monitoring vary and are adjusted in response to security incidents, to identify problems with security control implementations, or to evaluate system components that are determined to have a significant impact on security. Even given variations in assessment frequency, a continuous monitoring strategy supports system authorizations of a fixed frequency, including ongoing or on demand authorizations through thoughtful reuse of data with known latencies.

2.3 ROLE OF AUTOMATION IN CONTINUOUS MONITORING

When possible, organizations look for automated solutions to lower costs, enhance efficiency, and improve the reliability of monitoring security-related information. Security is implemented through a combination of people, processes and technology. The automation of IT security deals primarily with automating aspects of security that require little human interaction. This includes items such as verifying technical settings on individual network endpoints, or ensuring that the software on a machine is up to date with organizational policy. This automation serves to augment the security processes conducted by security professionals within an organization. Automation serves to reduce the amount of time a security professional must spend on doing redundant tasks thereby increasing the amount of time the trained professional may spend on tasks requiring human cognition.

While automation of IT security will significantly reduce the amount of time a human must spend doing certain tasks; it is not possible to automate all of an organization's IT security program functions. The technologies discussed in Appendix D, for example, still require human analysis for implementation and maintenance of the tools as well as appropriate interpretation of findings. Similarly, these tools operate within the context of processes designed, run and maintained by humans. If individuals carry out their responsibilities insecurely, then the effectiveness of the technologies is compromised and the security of the systems and the mission/business or organizational processes supported by those systems is put in jeopardy.

Consideration is given to continuous monitoring tools that:

[22] See NIST SP 800-37 for a discussion of authorization types.

- Pull information from a variety of sources (i.e., assessment objects[23]);
- Use open specifications such as the Security Content Automation Protocol (SCAP);
- Offer interoperability with other products such as help desk, inventory management, and incident response solutions;
- Support compliance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- Provide reporting with the ability to tailor output and drill down from high level metrics to system level measures; and
- Allow for data consolidation into Security Information and Event Management (SIEM) tools and dashboard products.

Automation makes security-related information readily available in an environment where monitoring needs change with threat activity. Therefore, during security control implementation (RMF Step 3), consideration is given to the capabilities inherent in available technology to support continuous monitoring as part of the criteria in determining how best to implement a given control.

Organizations' monitoring capabilities will expand and mature over time. Metrics will evolve with lessons learned and increases in organizational clarity around security status, and risk tolerance. The continuous monitoring strategy does not focus solely on the security-related information that is easy for an organization to collect or easy to automate. Implementation, effectiveness, and adequacy of all security controls are monitored along with organizational security status. When a continuous monitoring program is first implemented, there will likely be several aspects of the organization's security program that are manually monitored. The focus of a continuous monitoring strategy is to provide adequate information about security control effectiveness and organizational security status allowing organizational officials to make informed, timely security risk management decisions. Automation supports collecting more data more frequently and from a larger and more diverse pool of devices, systems, people and processes. It can therefore make comprehensive, ongoing control of security practical and affordable. The extent to which the monitoring effort is automated is dependent upon the maturity of the organization's monitoring capabilities. How effective the organization is in utilizing the monitoring results (obtained in a manual or automated fashion) still depends upon the organizational continuous monitoring strategy including validity and comprehensiveness of the metrics, as well as the processes in place to analyze monitoring results and respond to findings. Technologies for enabling automation of some continuous monitoring tasks are discussed in greater detail in Appendix D.

2.4 CONTINUOUS MONITORING ROLES AND RESPONSIBILITIES

This section describes the roles and responsibilities of key participants involved in an organization's continuous monitoring program.[24] Recognizing that organizations have widely varying missions and organizational structures, there may be differences in naming conventions

[23] See NIST SP 800-53A for information on assessment objects.

[24] Organizations may define other roles (e.g., systems administrator, common control provider) to support the continuous monitoring process.

for continuous monitoring-related roles and how specific responsibilities are allocated among organizational personnel (e.g., multiple individuals filling a single role or one individual filling multiple roles). Roles and responsibilities commonly associated with continuous monitoring include:

Risk Executive (Function). The risk executive (function) oversees the organization's continuous monitoring program. The risk executive (function) helps ensure that, individually and collectively, information system security considerations are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its mission/business processes. During the continuous monitoring process, the risk executive (function) maintains the organization's overall information security risk posture and risk tolerance based on the aggregated risk from each of the information systems and supporting infrastructures for which the organization is responsible. The risk executive (function) provides this information to the chief information officer, senior information security officer, information owners, and information system owners. The information is used to determine the continuous monitoring strategy that includes the criteria for the frequency with which security controls and metrics are monitored and when information systems should be reauthorized. The risk executive (function) reviews status reports and provides input to mission/system level entities on monitoring strategy and requirements, promotes collaboration and cooperation among organizational entities, facilitates sharing of security risk-related information among authorizing officials, provides an organization-wide forum to consider all sources of risk, and ensures that risk information is considered for continuous monitoring decisions.

Chief Information Officer (CIO). The CIO leads the organization's information security continuous monitoring program. The CIO ensures that an effective continuous monitoring program is established and implemented for the organization by establishing expectations and requirements for the organization's continuous monitoring program; working closely with authorizing officials to provide funding, personnel, and other resources to support continuous monitoring; and maintaining high-level communications and working group relationships among organizational entities.

Senior Information Security Officer (SISO). The SISO establishes, implements, and maintains the organization's continuous monitoring program; develops organizational program guidance (i.e., policies/procedures) for continuous monitoring of the security program and information systems; develops configuration management guidance for the organization; consolidates and analyzes POA&Ms to determine organizational security weaknesses and deficiencies; acquires or develops and maintains automated tools to support information systems continuous monitoring and ongoing authorizations; provides training on the organization's continuous monitoring program and process; and provides support to information owners/information system owners and common control providers on how to implement continuous monitoring for their information systems.

Authorizing Official (AO). The AO assumes responsibility for ensuring the organization's continuous monitoring program is applied with respect to a given information system. The AO ensures the security posture of the information system is maintained, reviews security status reports and critical security documents and determines if the risk to the organization from operation of the information system remains acceptable, determines whether significant information system changes require reauthorization actions, and reauthorizes the information system when required.

Information System Owner (ISO)/Information Owner/Steward. The ISO establishes processes and procedures in support of system level implementation of the organization's continuous monitoring program. This includes developing and documenting a continuous monitoring strategy for the information system; participating in the organization's configuration management process; establishing and maintaining an inventory of components associated with the information system; conducting security impact analyses on changes to the information system; conducting, or ensuring conduction of, assessment of security controls according to the continuous monitoring strategy; preparing and submitting security status reports in accordance with organizational policy and procedures; conducting remediation activities as necessary to maintain the current authorization status; revising the system level security control monitoring process as required; reviewing continuous monitoring reports from common control providers to verify that the common controls continue to provide adequate protection for the information system; and updating critical security documents based on the results of continuous monitoring.

Common Control Provider. The common control provider establishes processes and procedures in support of ongoing monitoring of common controls. The common control provider develops and documents a continuous monitoring strategy for assigned common controls; participates in the organization's configuration management process; establishes and maintains an inventory of components associated with the common controls; conducts security impact analyses on changes that affect the common controls; conducts, or ensures conduction of, assessments of the common security controls as defined in the continuous monitoring strategy; prepares and submits security status reports in accordance with organizational policy/procedures; conducts remediation activities as necessary to maintain the current authorization status; updates/revises the common security control monitoring process as required; updates critical security documents as changes occur; and distributes critical security documents to individual information owners/information system owners, and other senior leaders in accordance with organizational policy/procedures.

Information System Security Officer (ISSO). The ISSO supports the organization's continuous monitoring program by assisting the ISO in completing continuous monitoring responsibilities and by participating in the configuration management process.

Security Control Assessor. The security control assessor assesses information system or program management security controls for the organization's continuous monitoring program. The security control assessor develops a security assessment plan for each security control, submits the security assessment plan for approval prior to conducting assessments, conducts assessments of security controls as defined in the security assessment plan, updates the security assessment report as changes occur during continuous monitoring, and updates/revises the security assessment plan as needed.

CHAPTER THREE

THE PROCESS

Implementing a Continuous Monitoring Program

This chapter describes the process of continuous monitoring. It provides guidance on establishing an information security continuous monitoring strategy and implementing a continuous monitoring program organization-wide, including activities at the organization tier, mission/business tier and at the information system tier. A well designed information security continuous monitoring strategy encompasses security control assessment, security status monitoring, and security status reporting in support of timely risk-based decision making throughout the organization. The five tenets key to any continuous monitoring program described above in Chapter 2 and in Appendix G of NIST SP 800-37 are: configuration management and change control; security impact analysis; security control assessments; security status reporting; and active involvement of management. An organization's plans for action based on the data collected is as important (if not more important) than the process of collecting the data so that "ongoing control" might more accurately describe the actual process at work through the implementation of a continuous monitoring program. The process for continuous monitoring is described as follows:

- **Define** a continuous monitoring strategy based on risk tolerance that maintains clear visibility into assets and awareness of vulnerabilities and utilizes up-to-date threat information.
- **Establish** measures, metrics, and status monitoring and control assessment frequencies that convey organizational security status and detect changes to the organization's information infrastructure and environments of operation, maintain visibility into assets, awareness of vulnerabilities, knowledge of threats, and status of security control effectiveness in a manner that supports continued operation within established risk tolerances.
- **Implement** a continuous monitoring program to collect the data required for the predefined metrics and to report on findings; automate collection, analysis and reporting of data where possible.
- **Analyze** the data collected and **Report** findings, determining the appropriate response. It may be necessary to collect additional information to clarify or supplement existing monitoring data.
- **Respond** to findings with technical, management and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.
- **Review and Update** the monitoring program, adjusting the continuous monitoring strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities; further enable data driven control of the security of an organization's information infrastructure; and increase organizational resiliency.

This process is depicted below in Figure 3- 1.

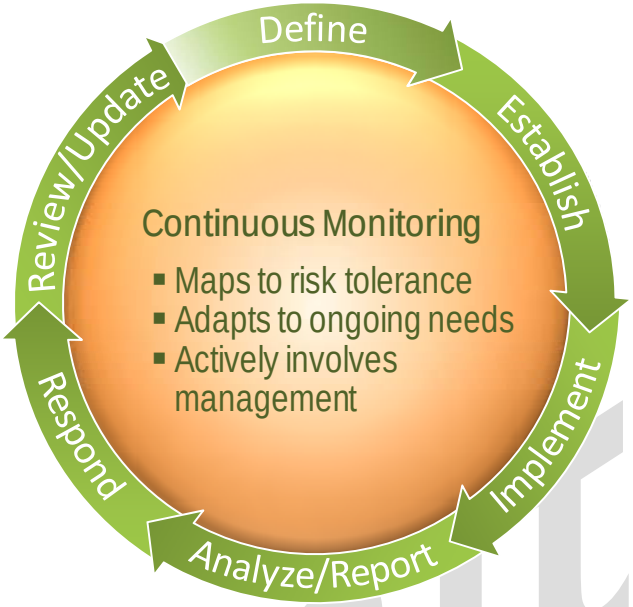

Figure 3 - 1. Continuous Monitoring Process

Risk tolerance, enterprise architecture, security architecture, security configurations, plans for changes to the enterprise architecture, and available threat information provide data that is fundamental to the execution of these steps and to ongoing management of information security-related risks. Security-related information related to actions of individuals and activities within individual systems, is analyzed for its relevance to organizational risk management at all three tiers.

The balance of this chapter discusses the process of continuous monitoring, providing detail on topics not covered by existing guidance and referencing existing guidance where appropriate. Primary roles, supporting roles, expected inputs, and expected outputs are given for each process step as a guide. Roles and responsibilities will vary across organizations as will implementation level details of a continuous monitoring program.

3.1 DEFINE CONTINUOUS MONITORING STRATEGY

An effective continuous monitoring program begins with development of a strategy that addresses continuous monitoring requirements and activities at each organizational tier (organization, mission/business, and information system). Depending on the organization, there may be overlap in the tasks and activities conducted at each tier. Each tier monitors security metrics and assesses security control effectiveness with established monitoring and assessment frequencies and status reports customized to support tier-specific decision making. Security control effectiveness can itself be taken as a security metric and as such have an associated status monitoring frequency. Continuous monitoring of security and risk is a challenging task in light of the constant organizational change with system additions, upgrades and decommissions, changes to operating environments, and the ever increasing quantity and sophistication of security threats. As such the key tenets described in Chapter 2 are threaded through the ensuing discussion of the execution of the continuous monitoring process. As changes occur, the continuous monitoring strategy is reviewed for relevancy, accuracy reflecting organizational risk tolerances, correctness of

measurements, and applicability of metrics. An inherent part of any continuous monitoring strategy is the inclusion of criteria describing the frequency and/or conditions that trigger review, update, and implementation of the monitoring strategy. Likewise, the organization defines criteria and procedures for updating the continuous monitoring program based on the revised continuous monitoring strategy.

3.1.1 ORGANIZATIONAL (TIER 1) AND MISSION/BUSINESS (TIER 2) CONTINUOUS MONITORING STRATEGY

The risk executive (function) determines the overall organizational risk tolerance and risk mitigation strategy at the organizational level. The continuous monitoring strategy and program are developed and implemented to support risk management in accordance with organizational risk tolerance. Typically, the organization-wide continuous monitoring strategy and program are developed at the organizational tier, with general procedures for implementation developed at the mission/business tier. If the strategy is developed at the mission/business tier, organizational officials at Tier 1 review and approve the strategy to ensure organizational risk tolerance across all missions and business processes has been appropriately considered. This information is communicated to staff at the mission, business and system levels and reflected in mission/business and system level policies and procedures.

At Tiers 1 and 2, the continuous monitoring strategy may include supporting policies, procedures and templates such as:

- Policy defining key metrics;
- Policy for modifications to and maintenance of the monitoring strategy;
- Policy and procedures for the assessment of security control effectiveness;
- Policy and procedures for security status monitoring;
- Policy and procedures for security status reporting (on control effectiveness and status monitoring);
- Policy and procedures for assessing risks and gaining threat information and insights;
- Policy and procedures for configuration management;
- Policy and procedures for security impact analysis;
- Policy and procedures for implementation and use of organization-wide tools;
- Policy and procedures for establishment of monitoring frequencies;
- Policy and procedures for determining sample sizes and populations and for managing object sampling;
- Procedures for determining security measures and data sources;
- Templates for assessing risks; and
- Templates for security status reporting (on control effectiveness and status monitoring).

Policies, procedures and templates necessarily address manual and automated monitoring methodologies. Additionally at these tiers, organizations establish policy and procedures for

training of personnel with continuous monitoring roles. This may include training on management and use of automated tools (e.g., establishing baselines and tuning of measurements to provide accurate monitoring of operational environments). It may also include training for recognition of and appropriate response to triggers and alerts from metrics indicating risks beyond acceptable limits, as well as training on internal or external reporting requirements. This training may be included in existing role-based training requirements for those with significant security roles, or it may consist of training specifically focused on implementation of the organization's continuous monitoring policy and procedures.

Tier 1 and 2 officials have responsibilities throughout the continuous monitoring process beginning with the development of the strategy:

- Provide input to the development of the organizational continuous monitoring strategy including establishment of measures, metrics, policies and procedures, compiling and correlating Tier 3 data into security-related information of use at Tiers 1 and 2, policies on assessment and monitoring frequencies, and provisions for ensuring sufficient depth and coverage when sampling methodologies are utilized [Define, Establish, Implement].
- Verify correct implementation of common and PM security controls (typically at Tier 2) [Implement].
- Review monitoring results (security-related information) to determine security status in accordance with organizational policies and definitions [Analyze/Report].
- Review new or modified legislation, directives, policies, etc. for any changes to security requirements [Review/Update].
- Review monitoring results to identify new information on vulnerabilities [Review/Update].
- Review of information on new or emerging threats as evidenced by threat activities present in monitoring results, threat modeling (asset and attack based), classified and unclassified threat briefs, USCERT reports, and other information available through trusted sources, interagency sharing, and external government sources [Review/Update].
- Analyze potential security impact to organization and mission/business functions resulting from changes to information systems and their environments of operation along with the security impact to the enterprise architecture resulting from the addition or removal of information systems [Analyze/Report].
- Make a determination as to whether or not current risk is within organizational risk tolerance levels [Analyze/Report, Review/Update].
- Take steps to respond to risk as needed (e.g., request new or revised measures and metrics, additional or revised assessments, modifications to existing common or PM security controls, or additional controls) [Respond].
- Update relevant security documentation [Respond].

Decisions and activities by Tier 1 and 2 officials may be constrained by things such as mission/business needs, limitations of the infrastructure (including the human components), immutable governance policies, and external drivers.

Primary Roles: Risk executive (function), Chief Information Officer, Senior Information Security Officer, Authorizing Officials

Supporting Roles: Information System Owner/Common Control Provider

Expected Input: Organizational risk assessment and current risk tolerance, current threat information, organizational expectations and priorities, available tools from OMB lines of business and/or third party vendors

Expected Output: Updated information on organizational risk tolerance, organization-wide continuous monitoring strategy and associated policies, procedures, templates, tools

3.1.2 INFORMATION SYSTEM (TIER 3) CONTINUOUS MONITORING STRATEGY

The Authorizing Official determines the risk of operating an individual system. The system-level continuous monitoring strategy and program are developed and implemented to support risk management, not only at the system level, but at *all three tiers* in accordance with system and organizational risk tolerance. System level security-related information includes assessment data *pertaining to* system level security controls and measures/metrics data *obtained from* system level security controls. System owners establish a system-level strategy for continuous monitoring, by considering factors such as the system's architecture and operational environment, as well as organizational and mission-level requirements, policies, procedures, and templates. Although the strategy and program may be defined at Tiers 1 or 2, system specific policies for implementation are developed at Tier 3. Systems owner are typically given some freedom in determining how best to customize tool use on their systems, comply with data calls and information requirements, and operate within established risk tolerances.

System-level monitoring addresses monitoring security controls for effectiveness (assessments), monitoring for security status, and reporting findings. At a minimum, all security controls are assessed for effectiveness in accordance with the system security plan, and the methods described in NIST SP 800-53A. System owners determine assessment frequencies of security controls based on drivers from all three tiers. A full discussion of factors to consider when determining assessment and monitoring frequencies can be found in section 3.3. System level security-related information is used to determine security status at all three tiers. Use of system level security-related information in metrics for determining security status is addressed in section 3.2.

The continuous monitoring strategy at the system level also supports ongoing authorization. Ongoing authorization implies recurring updates to the authorization decision information in accordance with assessment and monitoring frequencies. Assessment results from monitoring common controls implemented and managed at the organizational or mission/business level may be combined with information generated at the system level in order to provide the AO with a complete set of independently-generated evidence. [25] Assessment evidence obtained from continuous monitoring is, at a minimum, provided to AOs as often as required by organizational policy.

[25] See NIST SP 800-53, CA-2, Control Enhancement 1, for specific assessor independence requirements. Assessors need only be independent of the operation of the system. They may be from within the organizational tier, the mission/business tier, or from within some other independent entity internal or external to the organization. Results of assessments done by system operators can be used if they have been validated by independent assessors.

Tier 3 officials have responsibilities throughout the continuous monitoring process that include support of the development of the organizational strategy along with the tasks described in the RMF:

- Provide input to the development and implementation of the continuous monitoring strategy [Define, Establish, Implement; RMF Step 2].
- Support planning and implementation of security controls, the deployment of automation tools and how those tools interface with one another in support of the continuous monitoring strategy [Implement; RMF Step 2]
- Determine the security impact of changes to the information system and its environment of operation, including changes associated with commissioning or decommissioning the system [Analyze/Report; RMF Step 6].
- Assess ongoing security control effectiveness [Implement; RMF Step 4[26], RMF Step 6].
- Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones [Respond; RMF Step 6].
- Provide ongoing input to the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process [Respond; RMF Step 6].
- Report the security status of the information system including the data needed to inform Tier 1 and 2 metrics [Analyze/Report; RMF Step 4, RMF Step 6].
- Review the reported security status of the information system to determine whether the risk to the system and the organization remains within organizational risk tolerances [Analyze/Report; RMF Step 5, RMF Step 6].

Primary Roles: Information System Owner/Common Control Provider, Information System Security Officer

Supporting Roles: Senior Information Security Officer, Authorizing Official, Security Control Assessor

Expected Input: Organizational risk tolerance information, organizational continuous monitoring strategy, procedures and templates, system specific threat information, and system information (e.g., System Security Plan, Security Assessment Report, Plan of Action and Milestones, Security Assessment Plan, System Risk Assessment, etc.[27])

Expected Output: System-level continuous monitoring strategy that complements the Tier 1 and 2 strategies and the organizational security program and that provides security status information

[26] The RMF is a recurring process. Prior to initial authorization, the system is not included in the organization's continuous monitoring program. This reference to RMF 4 is relevant after the system becomes operational, and is passing through Step 4 leading into re-authorization.

[27] This system information comes out of RMF steps four, five, and six. Electronic, standardized templates and document management systems readily support frequent updates with data generated by continuous monitoring programs.

for all tiers and real-time updates to system authorization decision information as directed by the organizational continuous monitoring strategy

3.1.3 DEFINE SAMPLE POPULATIONS

Once the continuous monitoring strategy has been defined, organizations may find that collecting data from every object of every system within an organization may be impractical or cost prohibitive. Sampling is a methodology employable with both manual and automated monitoring that may make continuous monitoring more cost effective. Sampling is used rather than 100% inspection to reduce the number of inspections and associated data that must be analyzed. NIST SP 800-53A describes how to achieve satisfactory coverage when determining sample populations for the three named assessment methods: examine, interview and test. The guidance in NIST SP 800-53A for basic, focused and comprehensive testing addresses the need for a "representative sample of assessment objects" or a "sufficiently large sample of assessment objects". Statistical tools can be used to help quantify the "how many" in "representative" and "sufficiently large." A risk with sampling is that the sample population may fail to capture the variations in assessment outcomes that would be obtained from an assessment of the full population. This could result in an inaccurate view of security control effectiveness and organizational security status.

NIST 800-53A provides guidance to help address the general issue of sampling and particularly that of coverage. In selecting a sample population, the coverage attribute is satisfied through consideration of three criteria:

- **Types of objects** - ensure sufficient diversity of types of assessment objects;
- **Number of each type** - chose "enough" objects of each type to provide confidence that assessment of additional objects will result in consistent findings;
- **Specific objects per type assessed** - given all of the objects of relevance throughout the organization that could be assessed, include "enough" objects per type in your sample population to sufficiently to account for the known or anticipated variance in assessment outcomes).

Sample measurements are summarized into a statistic (e.g., sample mean) and the observed value compared with the allowable value as represented by organizational risk tolerance. Statistics calculated using random sampling can become less reliable predictors of the full population if the sample size (i.e., objects to be tested) is small.[28] As described in the NIST Engineering Statistics Handbook, when deciding how many objects to include in sample populations, the following are considered[29]:

- Desired information (what question will the measurements help answer)
- Cost and practicality of making the assessment

[28] The Central Limit Theorem is a key theorem that allows one to assume that a statistic (e.g., mean) calculated from a random sample has a normal distribution (i.e., bell curve) regardless of the underlying distribution from which individual samples are being taken. For small sample sizes (roughly less than 30) the normal distribution assumption only tends to be good if the underlying distribution from which random samples are being taken is close to normal.

[29] For detailed information on selecting sample sizes see http://www.itl.nist.gov/div898/handbook/ppc/section3/ppc333.htm.

- Information already known about the objects, organization, or operating environments
- Anticipated variability across the total population
- Desired confidence in resulting statistics and conclusions drawn about the total population

Ways to achieve "increased" or "further increased grounds for confidence that a control is implemented correctly and operating as intended" across the entire organization include asking more targeted questions, increasing the types of objects assessed, and increasing the number of each type of object assessed.

Random sampling is usually the best approach. Organizations may also target specific objects for assessment in addition to the random sample, using the above criteria. However, sampling methods other than random sampling are used with care to avoid introducing bias. Automated data collection and analysis can reduce the need for sampling.

Primary Roles: Information System Owner, Common Control Provider, Information System Security Officer, Security Control Assessor

Supporting Roles: Risk Executive (Function), Authorizing Official, Chief Information Officer, Senior Information Security Officer

Expected Input: Organizational and system-level policies and procedures on continuous monitoring strategy, measures and metrics, and the security assessment plan updated with assessment and monitoring frequencies

Expected Output: Security assessment plan documentation on acceptable sample sizes, security-related information

3.2 ESTABLISH MEASURES AND METRICS

Organizations determine measures and metrics to be used to evaluate and control ongoing risk to the organization. Measures include all the security-related information from assessments and monitoring produced by automated tools as well as manually generated security-related information. Metrics are measures that have been organized into meaningful information to support decision making. Metrics are developed for system-level data to make it meaningful in the context of mission/business or organizational risk management. Multiple measures may support one metric, and metrics may use measures acquired at different frequencies and therefore with varying data latencies. Metrics may be calculated from a combination of security status monitoring and security control assessment data. Similarly, a measure may be a representation of data collected from one or more security controls. Some examples of measures are the number and severity of vulnerabilities revealed and remediated, number of unauthorized components on a network, unauthorized activity, percentage of properly configured desktops, percentage of systems that have tested contingency plans within prescribed time frames, and number of employees who are current on awareness training requirements. Some examples of metrics are the risk tolerance thresholds for organizations, the risk score associated with a given system configuration, and the security score of a to-be architecture in the context of the existing architecture and business needs. The PM controls and related metrics are examined and tracked at Tiers 2 and 1. These controls address the establishment and management of the organization's

information security program. They are deployed organization-wide, support all information systems and may be implemented as common controls.

An example of a metric with associated measures is given in Table 3-1.

Table 3-1. Sample Metric and Related Measures at Each Tier

Sample Metric: Vulnerability Score	
Tier	Contributing Measures and Metrics
Tier 3	• # Patches installed since last scoring • # Patches made publically available since last scoring • # Patches installed on day released • # Patches installed using automated patch management tool • # Patches installed before testing • Are procedures in place for testing patches before installing • Do configuration management procedures include sufficient updates to key documents following patch installation • Is vulnerability scanning software installed • Is SISO trained in vulnerability identification • # of vulnerabilities exploited since last scoring for which patches were publically available o Time between patch release and exploit o # of exploits within 1 (week/day/hour) of release of patch …
Tier 2	• % of information systems used in support of mission/business function with system vulnerability scores above 7 • Is vulnerability scanning software installed on all systems used in support of mission/business function? • Are all relevant SISOs trained in vulnerability detection and management • Are related policies and procedures being followed across the mission/business • …
Tier 1	• % of organizational information systems with system vulnerability scores above 7 • Is vulnerability scanning software installed on all organizational systems? • Are all SISOs trained in vulnerability detection and management? • Are related policies and procedures being followed across the organization • …

In order to calculate the metric, associated controls and/or their objects are assessed and monitored with frequencies consistent with the timing requirements expressed in the metric. For detailed information on establishing measures and metrics, see NIST SP 800-55.

Primary Roles: Risk Executive (Function), Chief Information Officer, Senior Information Security Officer

Supporting Roles: Authorizing Officials, Information System Owner/Common Control Provider

Expected Input: Organizational risk assessment, organizational risk tolerance, current threat information, reporting requirements, current vulnerability information

Expected Output: Measures and metrics to convey security status and security control effectiveness at all three tiers, and to give recipients/users of reports visibility into assets, awareness of vulnerabilities and knowledge of threats

3.3 ESTABLISH MONITORING AND ASSESSMENT FREQUENCIES

Determining frequencies for security status monitoring and for security control assessments are critical functions of the organization's continuous monitoring program. Monitoring frequencies for metrics are established such that current security-related information is delivered to organizational officials often enough to enable informed risk management decision making. Security control assessment frequencies are established to meet organizational requirements for effectiveness tracking in support of ongoing authorization as well as to help prove validity of security status monitoring data collected from controls.[30] As organizations move towards increased automation, dashboards are more readily updated in real-time with security status information at all tiers and independent security control assessment data is used to support ongoing system authorization.

For some organizations, real-time dashboards and ongoing assessments are a shift away from the model of complete security control assessments conducted at a distinct point in time. For this shift to be constructive and effective from security, assurance, and resource use perspectives, organizations determine the frequencies with which *each* security control or control element is assessed for effectiveness and the frequencies with which *each* metric is monitored. A continuous monitoring program allows for regular and frequent updates to security-related information, use of the information in risk response decisions, and potential reuse of the information in updates to system authorization packages. Though monitoring and assessment frequencies are singularly determined, organizational officials still seek to use this datum of different latencies to create a holistic view of the security of each system as well as a view of the security of the enterprise architecture. As ongoing monitoring is overshadowed by ongoing control, the views are not static but are changing even as new data is collected, as metrics and assessments are updated, as results are analyzed, and as adjustments are made to respond to risk. Ideally, monitoring and assessment frequencies are only important in the context of how the data is used and questions such as *When did the system receive authorization to operate* or *When was the system last tested* become less meaningful and metrics such as *How resilient is the system* or *How long did it take to restore our organization-wide vulnerability score* can be answered, and information used effectively.

3.3.1 KEY CONSIDERATIONS IN DETERMINING ASSESSMENT AND MONITORING FREQUENCIES

Organizations take the following criteria into consideration when establishing monitoring frequencies for metrics or assessment frequencies for security controls:

- **Security control volatility**. Volatile security controls are assessed more frequently, whether the objective be establishing security control effectiveness or supporting calculation of a measure or metric.[31] Controls in the NIST SP 800-53 Configuration Management family are a good example of volatile controls. Information system configurations typically experience high rates of change. Unauthorized or unanalyzed changes in the system configuration often render the system vulnerable to exploits. Therefore, corresponding controls such as CM-6,

[30] For the sake of consistency and clarity, discussions herein reserve the term *assessment frequencies* for the frequency with which security control effectiveness is assessed and the term *monitoring frequencies* for the frequency with which security metrics are monitored. It is noted that security related information used in measures and metrics includes security control assessment data.

[31] Security control volatility is a measure of how frequently a control is likely to change over time subsequent to its implementation.

Configuration Settings, and CM-8, Information System Component Inventory, may require more frequent assessment and monitoring, preferably using automated, SCAP-validated tools that provide near real-time alerts and status. Conversely, controls such as PS-2, Position Categorization, or PS-3, Personnel Screening, (from the NIST SP 800-53 Personnel Security family of controls) are not volatile in most organizational settings. They tend to remain static over long periods and would therefore typically require less frequent assessment.

- **System categorizations/impact levels**. In general, security controls implemented on systems that are categorized as high impact are monitored more frequently than controls implemented on moderate impact systems, which are in turn monitored more frequently than controls implemented on low impact systems.

- **Security controls or specific assessment objects providing critical functions**. Security controls or assessment objects that provide critical security functions (e.g., log management server, firewalls) are candidates for more frequent monitoring. Additionally, individual assessment objects that support critical security functions and/or are deemed critical to the system (in accordance with the Business Impact Analysis[32]) or to the organization may be candidates for more frequent monitoring.

- **Security controls with identified weaknesses.** Existing risks documented in security assessment reports (SAR) are considered for more frequent monitoring to ensure that risks stay within tolerance. Similarly, controls documented in the POA&M as having weaknesses are monitored more frequently until remediation of the weakness is complete. Note that not all weaknesses require the same level of monitoring. For example, weaknesses deemed in the SAR to be of minor or low impact risk to the system or organization are monitored less frequently than a weakness with a higher impact risk to the system or organization.

- **Organizational risk tolerance.**[33] Organizations with a low tolerance for risk (e.g., organizations that process, store, or transmit large amounts of proprietary and/or personally identifiable information (PII), organizations with numerous high impact systems, organizations facing specific persistent threats) monitor more frequently than organizations with a higher tolerance for risk (e.g., organizations with primarily low and moderate impact systems that process, store, or transmit very little PII and/or proprietary information).

- **Threat information**.[34] Organizations consider current credible threat information, including known exploits and attack vectors, when establishing monitoring frequencies. For instance, if a specific attack is developed which exploits a vulnerability of an implemented technology, then temporary or permanent increases to the monitoring frequencies for related controls or metrics may help provide protection from the threat.

- **Vulnerability information**.[35] Organizations consider current vulnerability information with respect to information technology products when establishing monitoring frequencies. For

[32] See NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems,* May 2010.

[33] See NIST SP 800-39, DRAFT for more information on how to determine organizational risk tolerance.

[34] Threat information refers to types of attacks rather than specific threat actors. For current threat information, see http://capec.mitre.org/.

[35] For current vulnerability information, see http://nvd.nist.gov/.

instance, if a specific product manufacturer provides software patches monthly, an organization might consider conducting vulnerability scans on that product at least that often.

- **Risk assessment results**. Results from organizational and/or system specific assessments of risk (either formal or informal) are examined and taken into consideration when establishing monitoring frequencies. For instance, if a system-specific risk assessment identifies potential threats and vulnerabilities related to non-local maintenance (NIST SP 800-53, MA-4), the organization considers more frequent monitoring of the records kept on non-local maintenance and diagnostic activities. If a risk scoring scheme is in place at the organization, the risk scores may be used as justification to increase or decrease the monitoring frequencies of related controls.

- **Output of monitoring strategy reviews**. Review and adjustment of the monitoring strategy is covered in detail in section 3.7.

- **Automation capability/Resource Availability.** As automation capability or resources are added, organizations consider increasing affected monitoring frequencies. Similarly, if resource availability decreases, the organization considers adjusting affected monitoring frequencies to ensure that security-related information is appropriately analyzed while continuing to meet organizational risk management requirements.

- **Reporting requirements**. Reporting requirements do not drive the continuous monitoring strategy but may play a role in the frequency of monitoring. For instance, if OMB policy requires quarterly reports on the number of unauthorized components detected and corrective actions taken, the organization would monitor the system for unauthorized components at least quarterly.

Because many security controls in the NIST SP 800-53 catalog have multiple implementation requirements along with control enhancements that may also have multiple implementation requirements, it may be necessary to assess or monitor individual control requirements and/or control enhancements within a given control with differing frequencies. For instance, the control AC-2, Account Management, has ten separate requirements (a. through j.) within the base control that apply to all three control baselines, and four control enhancements [(1) through (4)] that apply to the moderate impact baseline. Monitoring frequencies will vary for the sub-requirements in accordance with the considerations discussed. AC-2a involves the identification of account types. For a typical information system, once the account types have been identified and documented, they are not likely to change very often, so AC-2a is a candidate for relatively infrequent assessment. AC-2h involves the deactivation of temporary accounts and accounts of terminated or transferred users. Since personnel regularly come and go, a typical organization would most likely assess AC-2h on a more frequent basis than AC-2a. AC-2 (3) requires that the system automatically disable accounts after a specified time period of inactivity. As an automated control and one with typically high volatility, AC-2 (3) is a candidate for relatively frequent monitoring and also may serve to automate some of the base control requirements so that they can be monitored more frequently in accordance with the organizational continuous monitoring strategy.

Organizations also consider related controls (as noted in NIST SP 800-53, as amended) when establishing assessment frequencies. For instance, if a given control is assessed monthly, related controls may be affected and may also need to be assessed with the same or similar frequency.

Some security monitoring tools are capable of reporting frequencies that provide data that is too granular to be actionable. As this trend continues, organizations, as a part of their continuous

monitoring strategies, develop dashboards to help make sense of the data collected and determine monitoring frequencies for metrics that integrate well with their organization's governance processes. Use of standards-based tools is essential for the ability to aggregate data to dashboards from multiple sources, multiple events, and using a diverse tool set on diverse technologies. This will allow for like comparisons to be made across these multiple technologies and tools. This is discussed further in Appendix D.

3.3.2 ORGANIZATION AND MISSION/BUSINESS LEVELS

A minimum frequency with which each security control or metric is assessed or monitored across all organizational systems and common controls based on the criteria described in 3.1.1 is established at the mission/business level. Common, hybrid, and system specific security controls are addressed by organization and mission/business level policy and procedures as are PM security controls. Common controls are often inherited by a large number of organizational systems. The aggregate criticality of such controls may require more frequent assessments than would similar controls responsible for protecting a single system. Additionally, determining the frequency for assessing common controls includes the organization's determination of the trustworthiness of the common control provider. Because the PM controls are information security program process-related and are not specific to information systems, they do not tend to be volatile and typically do not lend themselves well to automation. Still, the organization considers the volatility of each PM control as well as current threat information as it applies to the organization and the PM controls, when establishing assessment frequencies.

Primary Roles: Chief Information Officer, Senior Information Security Officer

Supporting Roles: Risk Executive (Function), Authorizing Officials, Common Control Provider, Information System Owner

Expected Input: Organizational risk assessment, organizational risk tolerance, current threat information, reporting requirements, current vulnerability information, output from monitoring strategy reviews

Expected Output: Organization-wide policies and procedures, recommended frequencies with which each security control and metric is assessed or monitored

3.3.3 SYSTEM LEVEL

At the system level, system owners review the minimum monitoring/assessment frequencies established by organization or mission/business level policy and determine if the minimum frequencies are adequate for a given information system. For some information systems, it may be necessary to assess specific controls or metrics with greater frequency than prescribed by the organization, again based on the criteria described in section 3.3.1. System owners also consider identification of specific system components that may require more frequent monitoring than other system components (e.g., public facing servers, boundary protection devices).

Primary Roles: Information System Owner, Information System Security Officer

Supporting Roles: Authorizing Official, Senior Information Security Officer, Information Owner/Steward

Expected Input: Organizational strategy and procedures with minimum frequencies, current threat information, reporting requirements, current vulnerability information, output from monitoring strategy reviews, security assessment plans

Expected Output: Security assessment plans updated to reflect the frequency with which each system specific security control is assessed and metrics are monitored

3.3.4 EVENT DRIVEN ASSESSMENTS

Events may occur that trigger the immediate need to assess security controls or verify security status outside of requirements expressed in the continuous monitoring strategy. This may require an assessment that is unplanned but of the type defined in the continuous monitoring strategy, or a customized assessment tailored to address an emerging need (e.g., a change in planned assessment or monitoring frequency). Organizations define criteria and thresholds for event driven assessments and the potential subsequent need for reauthorization. Organizations consider events such as incidents, new threat information, significant changes to systems and operating environments, new or additional mission responsibilities, and results of a security impact analysis or assessment of risk when defining criteria for event driven assessments.

Depending on the significance of the event, an event driven assessment may trigger one or more system reauthorizations. For example, if a Web application is added to a system, an existing continuous monitoring process that includes configuration management and control, security impact analysis, developmental vulnerability scans, etc., may be sufficient to assess controls implemented for the new Web application and the added risk to the organization while maintaining the existing authorization, and without the need for additional assessments and a specific reauthorization action. However, if an organization experiences an incident involving unauthorized access to/theft of PII from a particular system, an immediate full assessment, beyond any expressed in the continuous monitoring strategy, and reauthorization may be warranted.[36]

If a formal reauthorization action is initiated, the organization targets only the specific security controls affected by the changes and reuses previous assessment results wherever possible (i.e., as long as the assessment results meet reuse requirements established by the organization).

Primary Roles: Information System Owner/Common Control Provider, Authorizing Official, Information System Security Officer

Supporting Roles: Risk Executive (Function), Senior Information Security Officer, Security Control Assessor

Expected Input: Organizational risk assessment, organizational risk tolerance, current threat information, current vulnerability information, organizational priorities and expectations

Expected Output: Documented criteria and thresholds for event driven assessments/authorizations (e.g., significant change procedures, policy and procedures on event driven authorizations)

[36] Examples noted here are for illustrative purposes only.

3.4 IMPLEMENT A CONTINUOUS MONITORING PROGRAM

The tools, technologies, and methodologies used to implement a continuous monitoring program are dependent in part on the available infrastructure and the maturity of the organization's measurement program.[37] Data is collected as required for predefined metrics, security control assessments are conducted, and the security-related information generated is reported. *All* security controls - management, operational, and technical - are included in the organizational continuous monitoring program. Every control is monitored for effectiveness, and every control is subject to use in monitoring security status. Collection, analysis and reporting of data are automated where possible. Whether manual or automated, the data collected is assembled for analysis and reported to the organizational officials charged with correlating and analyzing it in ways that are relevant for risk management activities. As indicated in the examples in Table 3-1of section 3.2, this may mean taking elements of information from a variety of sources, collected at various points in time, and combining it in ways that are meaningful for the official receiving it at the time that it is requested. Part of the implementation stage of the continuous monitoring process is effectively organizing and delivering monitoring data in preparation for analysis.

Primary Roles: Information System Owner, Common Control Provider, Information System Security Officer, Security Control Assessor

Supporting Roles: Risk Executive (Function), Authorizing Official, Chief Information Officer, Senior Information Security Officer

Expected Input: Organizational and system-level policies and procedures on continuous monitoring strategy, measures and metrics, the security assessment plan updated with assessment and monitoring frequencies, and automation specifications

Expected Outputs: Security-related information

3.5 ANALYZE DATA AND REPORT FINDINGS

Organizations analyze the security-related information resulting from continuous monitoring. It may be necessary to collect additional data to supplement or clarify security-related information under analysis. Reports are provided to organizational officials. System and mission level staff report up as required by organizational/mission level policies and procedures. Reporting on additional metrics and/or assessment results may be required by higher level organizations such as OMB. Organizations define security status reporting requirements in the continuous monitoring strategy. This includes the specific staff/roles to receive continuous monitoring reports, the content and format of the reports, the frequency of reports, and any tools to be used.

Security-related information resulting from continuous monitoring is analyzed in the context of stated risk tolerances, the potential impact that vulnerabilities may have on organizational and mission/business processes, and the potential impact of mitigation options. Tier 3 officials report on findings, document any system-level mitigations made and/or provide recommendations to officials at Tiers 1 and 2. Organizational officials at Tiers 1 and 2 review Tier 3 findings to determine aggregate security status and the effectiveness and adequacy of *all controls* in meeting mission/business and organizational information security requirements. Information contained within a report will vary based on its recipient, frequency, purpose, supported tool sets, and

[37] See NIST SP 800-55 for more information on measurement programs.

metrics used. For example, the risk executive (function) may receive a general report on all systems annually and a detailed report on specific high impact systems quarterly. The reports provided to the CIO and SISO may contain more granular technical data on all systems quarterly, and the AO may receive monthly comprehensive reports on the systems for which s/he is responsible. The computer incident response team (CIRT) lead may receive exception reports when alerts are generated, and network administrators may review dashboards showing network activity that is updated every minute, with summary metrics that are updated hourly or daily.[38] Organizations may consider more frequent reports for specific controls with more volatility or on controls for which there have been weaknesses or lack of compliance. High frequency reporting can be facilitated by the implementation of automated monitoring and reporting tools (see Appendix D).

Organizations also define requirements for reporting results of controls, such as PM controls, that are not easily automated. "Manual" aspects of the continuous monitoring strategy also include specifics on staff/roles to receive the reports, content and format of the reports, and the frequency of the reporting. Organizations develop procedures for collecting and reporting assessment and monitoring results, including results that are derived via manual methods, and for managing and collecting information from POA&Ms to be used for frequency determination, status reporting and monitoring strategy revision.

Organizational officials review the analyzed reports to determine whether to conduct mitigation activities or to transfer, avoid/reject, or accept risk. In some cases, authorizing officials may determine that accepting some specific risk is preferable to implementing a mitigating response. The rationale for such determinations may include organizational risk tolerance, negative impact to business/mission processes, or cost-effectiveness or ROI of the implementation. Resolution of risk is documented in the Security Assessment Report.

Primary Roles: Risk Executive (Function), Chief Information Officer, Senior Information Security Officer; Authorization Officials, Security Control Assessors

Supporting Roles: Information System Owners, Common Control Providers, System Security Officers

Expected Input: Security-related information, organizational continuous monitoring strategy, reporting requirements, security-related information

Expected Output: Analysis of security status information for all tiers and updated system authorization decision information (System Security Plan, Security Assessment Report, Plan of Action and Milestones)

3.5.1 REPORT ON SECURITY CONTROL ASSESSMENTS

Organizations report on assessments of all implemented security controls for effectiveness in accordance with organizational requirements. Security-related information from assessments may be conveyed in templates or spreadsheets or collected and reported in an automated fashion. At the system level, security-related information from assessments directly supports authorization decisions and plans of action and milestones creation and tracking. Some security controls or elements of security controls, by definition, are security metrics (e.g., SI-4 Information System

[38] Reporting frequencies noted here are for illustrative purposes only.

Monitoring). Hence, assessing the effectiveness of these controls results in monitoring the security status of the related metric.

Primary Roles: System Owner, Common Control Provider, System Security Officer, Security Control Assessor

Supporting Roles: Risk Executive (Function), Chief Information Officer, Chief Information Security Officer, Authorizing Official

Expected Input: Security-related information (assessment results); organizational continuous monitoring policies and procedures; reporting requirements from the Authorizing Official, Chief Information Officer, Chief Information Security Officer, and/or Risk Executive (Function)

Expected Output: Reports on assessment results as required by organizational continuous monitoring policies and procedures and by the Authorizing Official in support of ongoing authorization (or re-authorization)

3.5.2 REPORT ON SECURITY STATUS MONITORING

Organizations develop procedures for reporting on security status monitoring. Security status data is derived from monitoring the metrics (as defined in the continuous monitoring strategy) across the organization using output generated by organization-wide tools (often implemented as common controls). The organization-wide tools may be part of a specific system or systems, but the security-related information generated is typically not system specific.

Primary Roles: System Owner, Common Control Provider, System Security Officer, Security Control Assessor

Supporting Roles: Risk Executive (Function), Chief Information Officer, Chief Information Security Officer, Authorizing Official

Expected Input: Security-related information (security status data); organizational continuous monitoring policies and procedures.; reporting requirements from the Authorizing Official, Chief Information Officer, Chief Information Security Officer, and/or Risk Executive (Function)

Expected Output: Reports on security status as required by organizational continuous monitoring policies and procedures and by the Authorizing Official in support of ongoing authorization (or re-authorization)

3.6 RESPOND TO FINDINGS

Security-related information obtained from monitoring is analyzed at each tier and the analysis is met with tier appropriate responses. At Tier 1, response to findings may result in changes to security policies around organizational governance. Tier 1's response may be constrained by the mission/business needs and the limitations of the enterprise architecture (including the human components), immutable governance policies, or other external drivers. At Tier 2, response to findings may include requests for additional security-related information, new or modified metrics, changes in mission/business or system level policies, procedures, and alerts or other status reporting and/or additions or modifications to common control implementations. The Tier 2 response may be constrained by organizational governance policies and strategies as well as mission/business goals and objectives and limitations of organizational resources and infrastructure. At Tier 3, response to findings may include implementation of additional controls,

modifications to previously implemented controls, removal of systems' authorization to operate, changes to the frequency of monitoring, and/or additional or more detailed analysis of security-related information. At Tier 3, mitigation strategies have a direct and immediate impact on system-level risk. System-level mitigations are made within constraints set by mission/business or organizational policies, requirements and strategies, to ensure that organizational processes are not negatively affected.

Response to findings at all tiers may also include risk acceptance, risk avoidance/rejection, or risk sharing/transfer.[39]

Response strategies may be implemented over a period of time, documenting implementation plans in the system's plan of action and milestones. As assessments are conducted in support of continuous monitoring and ongoing authorization, response to security control weaknesses revealed from assessments and updates to related documentation is also ongoing. As weaknesses are found, response actions are evaluated and any mitigation actions are conducted immediately or are added to the POA&M and key system documents are updated accordingly. Security controls that are modified, enhanced, or added during the continuous monitoring process are assessed to ensure that the new or revised controls are effective in their implementations. Going forward, monitoring and assessing of new or revised controls are included in the overall continuous monitoring strategy. Assessments in support of continuous monitoring and ongoing system authorization are conducted in accordance with NIST SP 800-53A, as amended. If the "Response" step in the continuous monitoring process does not result in the desired and anticipated improvement in organizational security posture, the problem could trace back to issues such as inadequate monitoring data, poor security control implementation, invalid metrics, insufficient threat information, or poor analysis or correlation of any of these factors. Even with real-time organization specific and system specific security-related information, both vulnerability and threat data is always evolving and will therefore always be incomplete

Primary Roles: System Owner, Common Control Provider, System Security Officer

Supporting Roles: Authorizing Official, Senior Information Security Officer, Information Owner/Steward

Expected Input: Reports on security status, reports on assessment results (e.g. security assessment reports), organizational and system level risk assessments, security assessment plans, system security plans, organizational procedures and templates

Expected Output: Mitigated weaknesses, updated system security information (e.g., system security plans, POA&Ms, security assessment reports), updated security status reports

3.7 REVIEW AND UPDATE THE MONITORING PROGRAM AND STRATEGY

Continuous monitoring strategies and programs are not static. Security control assessments, security status metrics, and monitoring and assessment frequencies change in accordance with the needs of the organization. The continuous monitoring program is reviewed to ensure that it sufficiently supports the organization in operating within acceptable risk tolerance levels, ensure that metrics remain relevant and that data is current and complete, identify ways to improve organizational insight into security posture, effectively support informed risk management

[39] For a detailed description of risk responses, see NIST SP 800-39.

decision making/ongoing authorizations, and improve the organization's ability to respond to known and emerging threats either through more timely identification and mitigation of vulnerabilities or more timely detection and recovery from attack.

The organization establishes a procedure for reviewing and modifying all aspects of the continuous monitoring strategy, including relevancy of the overall strategy, accuracy in reflecting organizational risk tolerance, accuracy/correctness of measurements, and applicability of metrics, reporting requirements, and monitoring and assessment frequencies. Factors precipitating changes in the monitoring strategy may include, but are not limited to:

- Changes to core missions or business processes;
- Significant changes in the enterprise architecture (including addition or removal of systems);
- Changes in organizational risk tolerance;
- Changes in threat information;
- Changes in vulnerability information;
- Changes within information systems (including changes in categorization/impact level);
- Increase/decrease in POA&Ms related to specific controls;
- Trend analyses of status reporting output; and
- New federal laws or regulations and/or
- Changes to reporting requirements.

Officials examine consolidated POA&M information to determine if there are common weaknesses/deficiencies among the organization's information systems and propose or request solutions. The aggregate POA&M information is used to allocate risk mitigation resources organization wide and to make adjustments to the monitoring strategy. Similarly, status reports and metrics are analyzed to determine if there are any security trends that suggest changes to the monitoring strategy may be necessary. For instance, if weekly assessments of component inventories over a six month period indicate that very few changes are being made in a given week and changes that *were* made are accurately reflected in the inventories, the organization may wish to reduce the frequency of monitoring component inventories to bi-weekly or monthly. Likewise, if bi-weekly audit record analyses over a six month period indicate increases in anomalous events, the organization may wish to increase the frequency of audit record reviews to weekly.

An organization's continuous monitoring strategy and program also change as the organization's security program(s) and monitoring capabilities mature. In a fully mature program, security-related information collection and analysis are accomplished using standardized methods across the organization, as an integral part of mission and business processes, and automated to the fullest extent possible. In this case, the security program is mature enough to ensure sufficient processes and procedures to effectively secure the enterprise architecture in accordance with organizational risk tolerances, and to collect, correlate, analyze and report on relevant security

metrics.[40] Continuous monitoring is a recursive process in the sense that the monitoring program and strategy are continually defined and refined as the steps of the process repeat. Further, the organization-wide application of continuous monitoring is accomplished through smaller or more narrowly focused instances of the similar efforts at the mission/business and systems tiers. In other words, the output of continuous monitoring at Tier 3 is input to the implementation of the continuous monitoring programs at Tiers 1 and 2. Working from the top of the pyramid in Figure 2-1 (Tier 1) to its bottom (Tier 3), upper tier monitoring strategies set the parameters for lower tier monitoring programs, and observations made at the lower tiers may result in changes to upper tier monitoring strategies. The continuous monitoring program itself must be monitored so that it can evolve with changes in organizational missions and objectives, operational environments and threats.

Primary Roles: Senior Information Security Officer, Authorizing Official, Information System Owner/Common Control Provider

Supporting Roles: Risk executive (function), Chief Information Officer, Information System Security Officer

Expected Input: Trend analyses from existing monitoring; organizational risk tolerance information; information on new laws, regulations, reporting requirements; current threat and vulnerability information; other organizational information as required, updates to automation specifications

Expected Output: Revised continuous monitoring strategy or a brief documented report noting review details and that modifications to the strategy were not necessary (in accordance with the established review process)

[40] See NIST SP 800-55, Rev.1 for more information on security metrics.

APPENDIX A

REFERENCES

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.

POLICIES, DIRECTIVES, INSTRUCTIONS

1. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, Management of Federal Information Resources, November 2000.
2. Office of Management and Budget Memorandum M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, October 2001.
3. Cyber Security Research and Development Act of 2002.

GUIDELINES

1. National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.
2. National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.
3. National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.
4. National Institute of Standards and Technology Special Publication 800-39, DRAFT, *Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View, December 2010*.
5. National Institute of Standards and Technology Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005.
6. National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.
7. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, June 2010.
8. National Institute of Standards and Technology Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security*, July 2008.
9. National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Log Management*, September 2006.
10. National Institute of Standards and Technology Special Publication 800-126, Revision 1, DRAFT, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1*, May 2010.
11. National Institute of Standards and Technology Special Publication 800-128, DRAFT, *Guide for Security Configuration Management of Information Systems*, March 2010.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

This appendix provides definitions for security terminology used within Special Publication 800-137. The terms in the glossary are consistent with the terms used in the suite of FISMA-related security standards and guidelines developed by NIST. Unless otherwise stated, all terms used in this publication are also consistent with the definitions contained in the CNSS Instruction 4009, *National Information Assurance Glossary*.

Activities	An assessment object that includes specific protection related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic).
Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.
Advanced Persistent Threats	An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.
Agency	See *Executive Agency*.
Allocation	The process an organization employs to determine whether security controls are defined as system-specific, hybrid, or common. The process an organization employs to assign security controls to specific information system components responsible for providing a particular security capability (e.g., router, server, remote sensor).

Application	A software program hosted by an information system.
Assessment	See *Security Control Assessment*.
Assessment Findings	Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a *satisfied* or *other than satisfied* condition.
Assessment Method	One of three types of actions (i.e., examine, interview, test) taken by assessors in obtaining evidence during an assessment.
Assessment Object	The item (i.e., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.
Assessment Objective	A set of determination statements that expresses the desired outcome for the assessment of a security control or control enhancement.
Assessment Procedure	A set of assessment *objectives* and an associated set of assessment *methods* and assessment *objects*.
Assessor	See *Security Control Assessor*.
Assurance	The grounds for confidence that the set of intended security controls in an information system are effective in their application.
Assurance Case [Software Engineering Institute, Carnegie Mellon University]	A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute.
Authentication [FIPS 200]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication.
Authorization (to operate)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Authorization Boundary [NIST SP 800-37]	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
Authorize Processing	See *Authorization*.
Authorizing Official (AO) [NIST SP 800-37]	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Authorizing Official Designated Representative [NIST SP 800-37]	An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Basic Testing	A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as black box testing.
Black Box Testing	See *Basic Testing*.
Categorization	The process of determining the security category (the restrictive label applied to classified or unclassified information to limit access) for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.
Chief Information Officer (CIO) [PL 104-106, Sec. 5125(b)]	Agency official responsible for: 1) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; 2) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and 3) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Chief Information Security Officer	See Senior Agency Information Security Officer.

Common Control [NIST SP 800-37]	A security control that is inherited by one or more organizational information systems. See Security Control Inheritance.
Common Control Provider [NIST SP 800-37, Rev. 1]	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).
Compensating Security Controls [NIST SP 800-53]	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.
Comprehensive Testing	A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as white box testing.
Computer Incident Response Team (CIRT)	Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability, or Cyber Incident Response Team).
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control (or Configuration Control) [CNSSI 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Continuous Monitoring	Maintaining ongoing awareness to support organizational risk decisions. See *Information Security Continuous Monitoring, Risk Monitoring* and *Status Monitoring.*
Controlled Interface	A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.
Controlled Unclassified Information	A categorical designation that refers to unclassified information that does not meet the standards for National Security classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces *Sensitive But Unclassified (SBU).*

Countermeasures [CNSSI 4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Cross Domain Solution	A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.
Coverage	An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (e.g., types of objects to be assessed and the number of objects to be assessed by type). The values for the coverage attribute, hierarchically from less coverage to more coverage, are basic, focused, and comprehensive.
Data Loss	The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.
Depth	An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. The values for the depth attribute, hierarchically from less depth to more depth, are basic, focused, and comprehensive.
Domain [CNSSI 4009]	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See *Security Domain*.
Dynamic Subsystem	A subsystem that is not continually present during the execution phase of an information system. Service-oriented architectures and cloud computing architectures are examples of architectures that employ dynamic subsystems.
Environment of Operation [NIST SP 800-37]	The physical surroundings in which an information system processes, stores, and transmits information.
Examine	A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time.
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
External Information System (or Component)	An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

External Information System Service	An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain arrangements.
Federal Agency	See *Executive Agency*.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
Federal Enterprise Architecture [FEA Program Management Office]	A business-based framework for government-wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.
Focused Testing	A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as gray box testing
Gray Box Testing	See *Focused Testing*.
High-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
Hybrid Security Control [NIST SP 800-53]	A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See *Common Control* and *System-Specific Security Control*.
Individuals	An assessment object that includes people applying specifications, mechanisms, or activities.
Industrial Control System	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.

Information [FIPS 199]	An instance of an information type.
Information Owner [CNSSI 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and /or information systems.
Information Security Architect	Individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.
Information Security Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
Information Security Policy [CNSSI 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information Security Program Plan [NIST SP 800-53]	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
Information Steward	Individual or group that helps to ensure the careful and responsible management of federal information belonging to the Nation as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to federal information to elements of the federal government and its customers, balanced by the obligation to protect the information in accordance with the provisions of FISMA and any associated security-related federal policies, directives, regulations, standards, and guidance.

Information System [44 U.S.C., Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Boundary	See *Authorization Boundary*.
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Engineer	Individual assigned responsibility for conducting information system security engineering activities.
Information System Security Engineering	Process that captures and refines information security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration.
Information System-related Security Risks	Information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. See *Risk*.
Information System Security Officer (ISSO) [CNSSI 4009]	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.
Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Interview	A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time.
Intrusion Detection and Prevention System (IDPS)	Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.
Joint Authorization	Security authorization involving multiple authorizing officials.
Low-Impact System [FIPS 200]	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
Management Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Measures	All the output produced by automated tools (e.g., IDS/IPS, vulnerability scanners, audit record management tools, configuration management tools, asset management tools) as well as various information security program -related data (e.g., training and awareness data, information system authorization data, contingency planning and testing data, incident response data). Measures also include security assessment evidence from both automated and manual collection methods.
Mechanisms	An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware) employed within or at the boundary of an information system.
Metrics	Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.
Moderate-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate, and no security objective is assigned a FIPS 199 potential impact value of high.

National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Net-centric Architecture	A complex system of systems composed of subsystems and services that are part of a continuously evolving, complex community of people, devices, information and services interconnected by a network that enhances information sharing and collaboration. Subsystems and services may or may not be developed or owned by the same entity, and, in general, will not be continually present during the full life cycle of the system of systems. Examples of this architecture include service-oriented architectures and cloud computing architectures.
Operational Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an Information system that are primarily implemented and executed by people (as opposed to systems).
Organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements).
Organizational Information Security Continuous Monitoring	Ongoing monitoring sufficient to ensure and assure effectiveness of security controls related to systems, networks, and cyberspace, by assessing security control implementation and organizational security status in accordance with organizational risk tolerance – and within a reporting structure designed to make real-time, data driven risk management decisions.
Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

Penetration Testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
Plan of Action & Milestones (POA&M) [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Reciprocity	Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Risk [FIPS 200, Adapted]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.]
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Risk executive (function) [NIST SP 800-37]	An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with organizational risks affecting mission/business success.
Risk Management	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Risk Monitoring	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Safeguards [CNSSI 4009]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Security Authorization	See *Authorization*.
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.
Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Security Control Assessor	The individual, group, or organization responsible for conducting a security control assessment.
Security Control Baseline [FIPS 200, Adapted]	One of the sets of minimum security controls defined for federal information systems in NIST Special Publication 800-53 and CNSS Instruction 1253.
Security Control Effectiveness	The measure of correctness of implementation (i.e., how consistently the control implementation complies with the security plan) and by how well the security plan meets organizational needs in accordance with current risk tolerance.
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.
Security Control Inheritance	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *Common Control*.
Security Domain [CNSSI 4009]	A domain that implements a security policy and is administered by a single authority.
Security Impact Analysis	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Management Dashboard [NIST SP 800-128]	A tool that consolidates and communicates information relevant to the organizational security posture in near-real time to security management stakeholders.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See *System Security Plan* or *Information Security Program Plan*.
Security Policy [CNSSI 4009]	A set of criteria for the provision of security services.

Security Posture	The security status of an enterprise's networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.
Security Requirements [FIPS 200]	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior (Agency) Information Security Officer (SISO) [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under the Federal Information Security Management Act (FISMA) and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information Security Officer* to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.
Senior Information Security Officer	See *Senior Agency Information Security Officer*.
Specification	An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system.
Status Monitoring	Monitoring the information security metrics defined by the organization in the information security continuous monitoring strategy.
Subsystem	A major subdivision of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
Supplementation (Assessment Procedures)	The process of adding assessment procedures or assessment details to assessment procedures in order to adequately meet the organization's risk management needs.
Supplementation (Security Controls)	The process of adding security controls or control enhancements to a security control baseline from NIST Special Publication 800-53 or CNSS Instruction 1253 in order to adequately meet the organization's risk management needs.
System	See *Information System*.

System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
System-Specific Security Control [NIST SP 800-37]	A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.
System Development Life Cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to the security control baseline. See *Tailoring*.
Tailoring [NIST SP 800-53, CNSSI 4009]	The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.
Tailoring (Assessment Procedures)	The process by which assessment procedures defined in Special Publication 800-53A are adjusted, or scoped, to match the characteristics of the information system under assessment, providing organizations with the flexibility needed to meet specific organizational requirements and to avoid overly-constrained assessment approaches.
Technical Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Test	A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time.
Threat [CNSSI 4009, Adapted]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Assessment [CNSSI 4009]	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

Threat Information	Information about types of attacks rather than specific threat actors.
Threat Source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
Vulnerability [CNSSI 4009]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment [CNSSI 4009]	Formal description and evaluation of the vulnerabilities in an information system.
White Box Testing	See *Comprehensive Testing*.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

AO	authorizing official
CIO	chief information officer
CIRT	computer incident response team
COTS	commercial off-the-shelf
DLP	Data Loss Prevention
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Act of 2002
IDPS	Intrusion detection and prevention system
ISO	Information system owner
ISSO	information system security officer
IT	information technology
NCP	National Checklist Program
NVD	National Vulnerability Database
OCIL	The Open Checklist Interactive Language
OMB	Office of Management and Budget
PII	personally identifiable information
PM	Program management
POA&M	plan of action & milestones
RMF	risk management framework
SAR	security assessment report
SCAP	Security Content Automation Protocol
SDLC	system development life cycle
SIA	security impact analysis
SIEM	security information and event management
SISO	senior information security officer
SP	special publication
USGCB	United States Government Configuration Baseline
XML	Extensible Markup Language

APPENDIX D

TECHNOLOGIES FOR ENABLING CONTINUOUS MONITORING

Organizations can make more effective use of their security budgets by implementing technologies to automate many of the continuous monitoring activities in support of organizational risk management policy and strategy, operational security, internal and external compliance, reporting, and documentation needs. There are a variety of tools and technologies available that an organization can use to efficiently and effectively gather, aggregate, analyze, and report data ranging from continuously monitoring the security status of its enterprise architecture and operating environment(s) down to components of individual information systems. These tools and technologies can enable and assist automated monitoring in support of a variety of organizational processes including:

- Ongoing assessments of security control effectiveness;
- Communication of security status at the appropriate level of granularity to personnel with security responsibilities;
- Management of risk and verification and assessment of mitigation activities;
- Assurance of compliance with high level internal and external requirements; and
- Analysis of the security impact of changes to the operational environment.

The tools and technologies discussed in this appendix leverage the strategies, policies, and roles and responsibilities of the overall continuous monitoring program, and can assist organizations in their efforts to automate the implementation, assessment, and monitoring of many NIST SP 800-53 security controls . Though these tools and technologies lend themselves primarily to the continuous monitoring of technical security controls that can be automated, they can provide evidence, in an automated manner, to support the existence and effectiveness of non-technical security controls or parts of technical security controls that cannot be easily automated. Automation is achieved through a variety of commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) products, built-in operating system capabilities, and custom tools and scripting that use standardized automation specifications.

It is important to understand and appreciate the need to assess the effectiveness of all security controls, particularly non-technical security controls, periodically. Data collected from automated tools may not provide feedback on the existence and the effectiveness of non-automated security controls. It may be possible in some cases to make certain inferences about the effectiveness of non-automated security controls based on data collected from automated tools. While it may not be possible to use automated tools and technologies to monitor adherence to policies and procedures, it may be possible to monitor associated security objectives in an automated fashion.

The Open Checklist Interactive Language (OCIL), discussed in section 4.3.1, may be used to partially automate certain controls that require human interaction and can be verified in a question and answer type format. For example, it may be possible to create an automated questionnaire to gather information related to annual security awareness training.

The validity of the security-related information collected continuously or on demand from today's automated tools assumes the continued effectiveness of the underlying management and operational security controls. As such, the value of automated tools and technologies, including those that perform direct data gathering and aggregation and analysis of data, is dependent upon the operational processes supporting their use. For organizations to realize the operational security benefits and for the tools and technologies to provide an accurate security status, knowledgeable staff should select, implement, operate, and maintain these tools and technologies, as well as all underlying security controls, interpret the monitoring data obtained, and select and implement appropriate remediation.

This appendix discusses the role of tools and technologies in automating many continuous monitoring activities. It discusses common tools, technologies, and open specifications used to collect, analyze, and meaningfully represent data in support of continuous monitoring of an organization's security risk posture, including providing visibility into the information assets, awareness of threats and vulnerabilities, and status of security control effectiveness. Examples of security controls that can be automated using the various technologies are included. This is not an exhaustive set of examples. New products and technologies continue to reach the market. Controls commonly automated but that do not appear as examples associated with the technologies named below include those where automation is achieved through capabilities built into operating systems, custom tools and scripts or a combination of several tools and capabilities.[41]

D.1 TECHNOLOGIES FOR SECURITY ENGINEERING AND DIRECT DATA GATHERING

Direct data gathering technologies are those that provide the capability to observe, detect, prevent, or log known security threats and vulnerabilities, and/or remediate or manage various aspects of security controls implemented to address those threats and vulnerabilities. These technologies are primarily implemented at the system level (Tier 3). However, they can be configured to support all of an organization's ongoing security monitoring needs up through mission/business processes and information security governance metrics. Tools and technologies implemented and configured to provide a security capability across an organization would be considered a common control.

A continuous monitoring domain is an IT Security area that includes a common grouping of tools, technologies, and data. Data within the domains is captured, correlated, analyzed, and reported to present the security status of the organization that is represented by the domains monitored. Security automation is the technology that enables the interoperability and flow of data between these domains. Monitoring capabilities are achieved through the use of a variety of tools and techniques. The granularity of the information collected is determined by the organization, based on its monitoring objectives and the capability of the enterprise architecture to support such activities.

This section describes eleven security automation domains that provide direct data gathering technologies:

[41] Examples of such controls that lend themselves to full or partial automation through security engineering or the use of proprietary/third party software and log management tools include account management, security training records, incident reporting and physical access control.

- Vulnerability Management
- Patch Management
- Event Management
- Incident Management
- Malware Detection
- Asset Management
- Configuration Management
- Network Management
- License Management
- Information Management
- Software Assurance

Figure 4-1. Continuous Monitoring Domains

The domains are pictured in Figure 4-1.

D.1.1 VULNERABILITY AND PATCH MANAGEMENT

A vulnerability is a software flaw that introduces a potential security exposure. The number of vulnerabilities and patches developed to address those vulnerabilities continues to grow, making manual patching of systems and system components an increasingly difficult task. To the extent possible, organizations should identify, report, and remediate vulnerabilities in a coordinated,

organization-wide manner using automated vulnerability and patch management tools and technologies.

Vulnerability scanners are commonly used in organizations to identify vulnerabilities on hosts and networks and on commonly used operating systems and applications. These scanning tools can proactively identify vulnerabilities, provide a fast and easy way to measure exposure, identify out-of-date software versions, validate compliance with an organizational security policy, and generate alerts and reports about identified vulnerabilities.

Patch management tools scan for vulnerabilities on systems and system components participating in an organization's patching solution, provide information regarding needed patches and other software updates on affected devices, and allow an administrator to decide on the patching implementation process. Patch management tools and utilities are available from various vendors to assist in the automated identification, distribution, and reporting of software patches. It is critical to understand the impact of patches before applying and to deploy them within the context of a defined patch management policy, providing assurances that systems will not lose critical functionality due to an unintended side effect of a patch. In some cases where a patch cannot be deployed, other compensating security controls may be necessary.

The implementation and effective use of vulnerability assessment and patch management technologies[42] can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including SI-2, Flaw Remediation; CA-2, Security Assessments; CA-7, Continuous Monitoring; CM-3, Configuration Change Control; IR-4, Incident Handling; IR-5, Incident Monitoring; MA-2, Controlled Maintenance; RA-5, Vulnerability Scanning; SA-11, Developer Security Testing; and SI-11, Error Handling. Vulnerability assessment and patch management technologies may also provide supporting data to assist organizations in responding to higher level reporting requirements in the areas of configuration and vulnerability management.

D.1.2 EVENT AND INCIDENT MANAGEMENT

Event management involves monitoring and responding to as necessary, observable occurrences in a network or system. A variety of tools and technologies exist to monitor events, such as intrusion detection systems and logging mechanisms. Certain events may signal that an incident has occurred, which is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. Incident management tools may assist in detecting, responding to, and limiting the consequences of a malicious cyber attack against an organization.

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or system component. Many logs within an organization contain records related to computer security. These computer security logs can be generated by many sources, including security software such as malware protection software, firewalls, and intrusion detection and prevention systems, operating systems on servers, workstations, networking equipment, and applications.

[42] For more information, please refer to NIST Special Publication 800-40 Version 2.0, *Creating a Patch and Vulnerability Management Program*, November 2005.

The number, volume, and variety of security logs have increased greatly, which has created the need for information system security log management – the process of generating, transmitting, storing, analyzing, and disposing of security log data. Log management[43] is essential for ensuring that security records are stored in sufficient detail for an appropriate period of time. Logs are a useful resource when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems, and as such, supports a continuous monitoring capability.

The implementation and effective use of logging and log management tools and technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including 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; CA-2, Security Assessments; CA-7, Continuous Monitoring; IR-5, Incident Monitoring; RA-3, (Risk Assessment; and SI-4, Information system Monitoring.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. *Intrusion prevention* is the process of performing intrusion detection and attempting to stop possible incidents as they are detected. Intrusion detection and prevention systems (IDPS)[44] are focused primarily on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators for further analysis and action.

IDPSs typically are used to record information related to observed events, notify security administrators of important observed events, and automatically generate reports, with remediation actions performed manually after human review of the report. Many IDPSs can also be configured to respond to a detected threat using a variety of techniques, including changing the security environment (e.g., reconfiguring a firewall) or blocking the attack.

Within the context of a continuous monitoring program, IDPSs can be used to supply evidence of the effectiveness of security controls (e.g., policies, procedures, and other implemented technical controls), document existing threats, and deter unauthorized use of individual information systems. The implementation and effective use of IDPSs can also assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including AC-4, Information Flow Enforcement; AC-17, Remote Access; AC-8, Wireless Access; AU-2, Auditable Events; AU-6, Audit Review, Analysis, and Reporting; AU-12, Audit Generation; AU-13, Monitoring for Information Disclosure; CA-2, Security Assessments; CA-7, Continuous Monitoring; IR-5, Incident Monitoring; RA-3, Risk Assessment; SC-7, Boundary Protection; SI-3, Malicious Code Protection; SI-4, Information System Monitoring; and SI-7, Software and Information Integrity. IDPSs may also provide supporting

[43] For more information, please refer to NIST Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006.

[44] For more information, please refer to NIST Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007.

data to assist organizations in meeting US-CERT incident reporting requirements and in responding to OMB and agency CIO reporting requirements in the areas of system and connections inventory, security incident management, boundary protections, and configuration management.

D.1.3 MALWARE DETECTION

Malware detection[45] provides the ability to identify and report on the presence of viruses, Trojan horses, spyware, or other malicious code on or destined for a target system. Organizations typically employ malware detection mechanisms at information system entry and exit points (e.g., firewalls, email servers, Web servers, proxy servers, remote access servers) and at endpoint devices (e.g., workstations, servers, mobile computing devices) on the network to detect and remove malicious code transported by electronic mail, electronic mail attachments, Web accesses, removable media or other means, or inserted through the exploitation of information system vulnerabilities.

Malware detection mechanisms can be configured to perform periodic scans of information systems, as well as real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy. Malware detection mechanisms can frequently take a predetermined action in response to malicious code detection.

In addition to malware detection, a variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Used in conjunction with configuration management and control procedures and strong software integrity controls, malware detection mechanisms can be even more effective in preventing execution of unauthorized code. Additional risk mitigation measures, such as secure coding practices, trusted procurement processes, and regular monitoring of secure configurations, can help ensure that unauthorized functions are not performed.

The implementation and effective use of malware detection technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls, including CA-2, Security Assessments; CA-7, Continuous Monitoring; IR-5, Incident Monitoring; RA-3, Risk Assessment; SA-12, Supply Chain Protection; SA-13, Trustworthiness; SI-3, Malicious Code Protection; SI-4, Information System Monitoring; SI-7, Software and Information Integrity; and SI-8, Spam Protection. Malware detection technologies may also provide supporting data to assist organizations in meeting US-CERT incident reporting requirements and in responding to OMB and agency CIO reporting requirements related to incident management, remote access, and boundary protections.

D.1.4 ASSET MANAGEMENT

Asset management tools maintain inventory and change management of software and hardware within the organization. It may be a combination of system configuration, network management, and license management tools, or a special purpose tool. Asset management software tracks the lifecycle of an organization's assets and provides tools such as remote management of assets and various automated management functions.

The implementation and effective use of asset management technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP

[45] For more information, please refer to NIST Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005.

800-53 security controls including CA-7, Continuous Monitoring; CM-2, Baseline Configuration; CM-3, Configuration Change Control; CM-4, Security Impact Analysis; CM-8, Information System Component Inventory; and SA-10, Developer Configuration Management.

D.1.5 CONFIGURATION MANAGEMENT

Configuration management tools allow administrators to configure settings, monitor changes to settings, collect setting status, and restore settings as needed. Managing the numerous configurations found within information systems and network components has become almost impossible using manual methods. Automated solutions may lower cost of configuration management efforts while enhancing efficiency and improving reliability.

System configuration scanning tools provide the automated capability to audit and assess a target system to determine its compliance with a defined secure baseline configuration. A user may confirm compliance and identify deviations from checklists appropriate for relevant operating systems and/or applications.

If an information system or system component is unknowingly out of synchronization with the approved secure configurations as defined by the organization's baseline configurations and the System Security Plan, organization officials and system owners may have a false sense of security. An opportunity to take actions that would otherwise limit vulnerabilities and help protect the organization from attack would subsequently be missed. Monitoring activities offer the organization better visibility into the state of security for its information systems, as defined by the security metrics being monitored.

Identity and account configuration management tools allow an organization to manage identification credentials, access control, authorization, and privileges. Identity management systems may also enable and monitor physical access control based on identification credentials. Identity and account configuration management tools often have the ability to automate tasks such as account password resets and other account maintenance activities. These systems also monitor and report on activities such as unsuccessful login attempts, account lockouts, and resource access.

There are a wide variety of configuration management tools available to support an organization's needs. When selecting a configuration management tool, organizations should consider tools that can pull information from a variety of sources and components. Organizations should choose tools that are based on open specifications such as SCAP; that support enterprise interoperability, assessment, and reporting; that provide the ability to tailor and customize output; and that allow for data consolidation into SIEM tools and management dashboards.

The implementation and effective use of configuration management technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including 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; CA-2, Security Assessments; CA-7, Continuous Monitoring; CM-2, Baseline Configuration; CM-3, Configuration Change Control; CM-5, Access Restrictions for Change; CM-6, Configuration Settings; CM-7, Least Functionality; 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); IR-5, Incident Monitoring; MA-5, Maintenance Personnel; PE-3,

Physical Access Control; RA-3, Risk Assessment; SA-10, Developer Configuration Management; and SI-2, Flaw Remediation. Enterprise security configuration management and engineering technologies may also provide supporting data to assist organizations in responding to higher level compliance reporting requirements in the areas of configuration and asset management.

D.1.6 NETWORK MANAGEMENT

Network configuration management tools include host discovery, inventory, change control, performance monitoring, and other network device management capabilities. Some network configuration management tools automate device configuration and change management and validate device compliance against pre-configured policies.

The implementation and effective use of network management technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including AC-4, Information Flow Enforcement; AC-17, Remote Access; AC-18, Wireless Access; CA-7, Continuous Monitoring; CM-2, Baseline Configuration; CM-3, Configuration Change Control; CM-4, Security Impact Analysis; CM-6, Configuration Settings; CM-8, Information System Component Inventory; SC-2, Application Partitioning; SC-5, Denial of Service Protection; SC-7, Boundary Protection; SC-10, Network Disconnect; SC-32, Information System Partitioning; and SI-4, Information System Monitoring.

D.1.7 LICENSE MANAGEMENT

Similarly to systems and network devices, software and applications are also a relevant data source for continuous monitoring. Software asset and licensing information may be centrally managed by a software asset management tool to track license compliance, monitor usage status, and manage the software asset lifecycle. License management tools offer a variety of features to automate inventory, utilization monitoring and restrictions, deployment, and patches for software and applications.

The implementation and effective use of license management technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including CA-7, Continuous Monitoring; CM-8, Information System Component Inventory; and SA-6, Software Usage Restrictions.

D.1.8 INFORMATION MANAGEMENT

There are vast quantities of digital information stored across the myriad of systems, network devices, databases, and other assets within an organization. Managing the location and transfer of information is essential to protecting the confidentiality, integrity, and availability of the data.

Data loss is the exposure of proprietary, sensitive, or classified information through either data theft or data leakage. Data theft occurs when data is intentionally stolen or exposed, as in cases of espionage or employee disgruntlement. Data leakage is the inadvertent exposure of data, as in the case of a lost or stolen laptop, an employee storing files using an Internet storage application, or an employee saving files on a USB drive to take home.

An effective data loss prevention (DLP) strategy includes data inventory and classification; data metric collection; policy development for data creation, use, storage, transmission, and disposal; and tools to monitor data at rest, in use, and in transit. There are a variety of tools available for DLP. Typical network and security tools such as network analysis software, application firewalls, and intrusion detection and prevention systems can be used to detect data and its

contents as its transmitted. There are also special purposed DLP software including features such as port and endpoint control, disk and file encryption, and database transaction monitoring. These tools may be specialized network traffic monitors or software agents installed on desktops, laptops, and servers. DLP tools have built-in detection and mitigation measures such as alerting via email, logging activities, and blocking transmissions.

The implementation and effective use of DLP technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including AC-4, Information Flow Enforcement; AC-17, Remote Access; CA-3, Information System Connections; CA-7, Continuous Monitoring; CM-7, Least Functionality; and SI-12, Information Output Handling and Retention.

D.1.9 SOFTWARE ASSURANCE

The NIST Software Assurance Metrics and Tool Evaluation (SAMATE) project defines software assurance as the "planned and systematic set of activities that ensures that software processes and products conform to requirements, standards and procedures from NASA Software Assurance Guidebook and Standard to help achieve:

- Trustworthiness – No exploitable vulnerabilities exit, either of malicious or unintentional origin
- Predictable Execution – Justifiable confidence that software, when executed, functions as intended."

There are several automation specifications that can assist with continuous monitoring of software assurance, including the emerging Software Assurance Automation Protocol (SwAAP) that is being developed to measure and enumerate software weaknesses and assurance cases. SwAAP uses a variety of automation specifications such as the Common Weakness Enumeration (CWE), which is a dictionary of weaknesses that can lead to exploitable vulnerabilities (i.e. CVEs) and the Common Weakness Scoring System (CWSS) for assigning risk scores to weaknesses. SwAAP also uses the Common Attack Pattern Enumeration & Classification (CAPEC), which is a publicly available catalog of attack patterns with a comprehensive schema and classification taxonomy, to provide descriptions of common methods for exploiting software and the Malware Attribute Enumeration & Characterization (MAEC), which provides a standardized language for encoding and communicating information about malware based upon attributes such as behaviors, artifacts, and attack patterns.

There are a number of software assurance tools and technologies that are now incorporating many of these automation specifications to provide software security throughout the software development lifecycle. The implementation and effective use of software assurance technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including CA-7, Continuous Monitoring; SA-4, Acquisitions; SA-8, Security Engineering Principles; SA-11, Developer Security Testing; ; SA-12, Supply Chain Protection; SA-13, Trustworthiness; SA-14, Critical Information System Components; and SI-13, Predictable Failure Prevention.

D.2 TECHNOLOGIES FOR AGGREGATION AND ANALYSIS

Aggregation and analysis technologies are those that have the capability to collect raw data from one or more security controls or other direct data gathering technologies and correlate, analyze, and represent the raw data in a way that provides a more meaningful perspective on the

effectiveness of security control implementation across part or all of an organization than would data from any single technology.

This section discusses common types of aggregation and analysis technologies and their role in supporting a continuous monitoring capability. They include SIEM and management dashboards.

D.2.1 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

To enhance the ability to identify inappropriate or unusual activity, organizations may integrate the analysis of vulnerability scanning information, performance data, network monitoring, and system audit record (log) information through the use of SIEM tools. SIEM tools are a type of centralized logging software that can facilitate aggregation and consolidation of logs from multiple information system components. SIEM tools can also facilitate audit record correlation and analysis. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of the vulnerability scans and correlating attack detection events with scanning results.

SIEM products usually include support for many types of audit record sources, such as operating systems, application servers (e.g., Web servers, email servers), and security software, and may even include support for physical security control devices such as badge readers. An SIEM server analyzes the data from all the different audit record sources, correlates events among the audit record entries, identifies and prioritizes significant events, and can be configured to initiate responses to events.

For each supported audit record source type, SIEM products typically can be configured to provide functionality for categorization of the most important audit record fields (e.g., the value in field 12 of application XYZ's logs signifies the source IP address) which can significantly improve the normalization, analysis, and correlation of audit record data. The SIEM software can also perform event reduction by disregarding those data fields that are not significant to information system security, potentially reducing the SIEM software's network bandwidth and data storage usage.

The implementation and effective use of SIEM technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including AC-5, Separation of Duties; AU-2, Auditable Events; AU-6, Audit Review, Analysis, and Reporting; AU-7, Audit Reduction and Report Generation; CA-2, Security Assessments; CA-7, Continuous Monitoring; IR-5, Incident Monitoring; PE-6, Monitoring Physical Access; RA-3, Risk Assessment; RA-5, Vulnerability Scanning; and SI-4, Information System Monitoring.

D.2.2 MANAGEMENT DASHBOARDS

A security management dashboard (or security information management console) consolidates and communicates information relevant to the organizational security status in near-real time to security management stakeholders. Personnel with responsibility for information security range from a technical system administrator, to the CISO, to the risk executive (function). The security management dashboard presents information in a meaningful and easily understandable format that can be customized to provide information appropriate to those with specific roles and responsibilities within the organization.

To maximize the benefits of management dashboards, it is important to obtain acceptance and support from upper-level management, define useful and quantifiable organization-specific performance metrics that are supported by information security policies and procedures, and ensure the availability of meaningful performance data.

The implementation and effective use of management dashboards can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including AC-5, Separation of Duties; CA-6, Security Authorization, CA-7, Continuous Monitoring; PM-6, Information Security Measures of Performance; PM-9, Risk Management Strategy; RA-3, Risk Assessment; and SI-4, Information System Monitoring.

D.3 AUTOMATION AND DATA SOURCES

Managing the security of systems throughout an enterprise is challenging for several reasons. Most organizations have many systems to patch and configure securely, with numerous pieces of software (operating systems and applications) to be secured on each system. Organizations need to conduct continuous monitoring of the security configuration of each system and be able to determine the security posture of systems and the organization at any given time. Organizations may also need to demonstrate compliance with security requirements expressed in legislation, regulation, and policy. All of these tasks are extremely time-consuming and error-prone because there has been no standardized, automated way of performing them. Another problem for organizations is the lack of interoperability across security tools; for example, the use of proprietary names for vulnerabilities or platforms creates inconsistencies in reports from multiple tools, which can cause delays in security assessment, decision-making, and vulnerability remediation. Organizations need standardized, automated approaches to overcoming these challenges

Automation is an efficient way to enable continuous monitoring within and across domains to capture, correlate, analyze, and report the overall security status of the organization. Automation technologies enable the interoperability and flow of data between these domains. Just about every security tool provides some sort of automated capability as part of its functionality, including importing and exporting data and performing other pre-configured, unassisted operations. Some of these automated capabilities rely on proprietary methods and protocols, while others use standardized specifications and methods. Some examples of security automation activities include:

- Scanning for vulnerabilities and automatically applying the appropriate patches;
- Automatically enabling security configurations based on a checklist of security settings;
- Scanning for compliance against a pre-configured checklist of security settings; and
- Collecting security metrics and measurements from tools and reporting them to a management console in a standardized format.

These are just a few of the many security activities that can be automated. The tools and technologies discussed in this publication leverage a variety of supporting protocols, specifications, and resources to provide the security management and monitoring standardization and interoperability necessary to enable continuous monitoring.

The automation specification movement is a community driven effort to standardize the format and nomenclature for communicating security and IT related information. These data exchange standards create the foundation for automating activities across disparate vendor tool sets, as well as interoperability across domain boundaries. The most mature and widely used set of specifications is the Security Content Automation Protocol (SCAP), which is used to standardize the communication of software flaws and security configurations. This section discusses how SCAP, the National Vulnerability Database (NVD) and security configuration checklists are used to represent and communicate data in a standardized format for performing security automation capabilities and their roles in supporting a continuous monitoring program.

D.3.1 SECURITY CONTENT AUTOMATION PROTOCOL (SCAP)

SCAP is a suite of specifications[46] that standardizes the format and nomenclature by which security software products communicate security flaw and security configuration information. SCAP is a multi-purpose protocol that supports automated vulnerability and patch checking, security control compliance activities, and security measurement. Goals for the development of SCAP include standardizing system security management, promoting interoperability of security products, and fostering the use of standard expressions of security content. SCAP can be used for maintaining the security of enterprise systems, such as automatically verifying the installation of patches, checking system security configuration settings, and examining systems for signs of compromise.

What Can Be Automated With SCAP

There are many readily available tools that can be used to automate continuous monitoring activities using SCAP. The SCAP Product Validation Program[47] is designed to test the ability of products to use the features and functionality available through SCAP and its component standards.

The SCAP validation program validates two types of vulnerability and patch scanners: authenticated and unauthenticated. Authenticated vulnerability and patch scanners provide the capability to scan a target system using target system logon privileges, to locate and identify the presence of known vulnerabilities and evaluate the software patch status to determine the ongoing security status of the system based on an organization's defined patch policy. Unauthenticated vulnerability scanners provide the capability to determine the presence of known vulnerabilities by evaluating the target system over the network without authenticated access. SCAP-enabled vulnerability scanners can be configured to scan connected systems at regular intervals, thus providing a quantitative and repeatable measurement and scoring of software flaws across systems. The use of SCAP-validated vulnerability scanners enables interoperability among vulnerability scanners and reporting tools to provide consistent detection and reporting of these flaws and supports comprehensive remediation tool capabilities.

While patching and vulnerability monitoring and remediation can often appear an overwhelming task, consistent mitigation of system software vulnerabilities can be achieved through a tested and integrated patching process. A mature patch and vulnerability management program that

[46] For more information please refer to NIST DRAFT Special Publication 800-126, Rev.1, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1*, May 2010.

[47] For more information on the SCAP Validation Program, please refer to http://scap.nist.gov/validation/.

embraces security automation technologies will help the organization be more proactive than reactive with regard to maintaining appropriate levels of security for their systems.

Vulnerability assessment and patch management technologies focus primarily on testing for the presence of known vulnerabilities in common operating systems and applications. For custom software and applications and in ferreting out unknown, unreported or unintentional vulnerabilities in commercial off-the-shelf (COTS) products, vulnerability assessment and analysis may require the use of additional, more specialized techniques and approaches, such as Web-based application scanners, source code reviews, and source code analyzers. These tools, coupled with security control assessment methodologies such as red team exercises and penetration testing, provide additional means for vulnerability identification.

The SCAP Validation Program evaluates the capabilities of configuration scanners that can audit and assess a target system to determine its compliance with a defined secure baseline configuration. Examples of secure baseline configurations include the Federal Desktop Core Configuration (FDCC)[48] and profiles created under the United States Government Configuration Baseline (USGCB)[49] initiative.

How to Implement SCAP

To implement SCAP for continuous monitoring, SCAP-validated[50] tools and SCAP-expressed checklists are used to automate secure configuration management and produce assessment evidence for many NIST SP 800-53 security controls. SCAP-expressed checklists can be customized as appropriate to meet specific organizational requirements. SCAP-expressed checklists can also map individual system security configuration settings to their corresponding security requirements. For example, mappings are available between Windows XP secure baseline configurations and the security controls in NIST SP 800-53. These mappings can help demonstrate that the implemented settings provide adequate security and adhere to requirements. The mappings are embedded in SCAP-expressed checklists which allow SCAP-validated tools to generate assessment and compliance evidence automatically. This can provide a substantial savings in effort and cost of configuration management. If SCAP-validated tools are not available or are not currently deployed within an organization, organizations should consider implementing SCAP-expressed checklists for their secure baseline configurations in order to be well-positioned when SCAP-validated tools become available and/or are deployed.

To automate continuous monitoring of known software vulnerabilities, SCAP-expressed checklists and SCAP-validated tools can be used to assess the software assets installed and derive a mitigation strategy for known vulnerabilities based on risk severity. By performing regularly scheduled scans of the enterprise architecture with the latest available SCAP-expressed security-related information, a security officer and/or system administrator can attain near real-time situational awareness of the security of their networked systems in terms of configuration settings and mitigation of known software vulnerabilities.

[48] For more information on the FDCC, please refer to http://fdcc.nist.gov.

[49] For more information on the USGCB, please refer to http://usgcb.nist.gov.

[50] For more information on SCAP validated products please refer to http://nvd.nist.gov/scapproducts.cfm.

Partially Automated Controls

The implementation, assessment and monitoring of some security controls may not be automated by existing tools; however they may be partially automated using the Open Checklist Interactive Language (OCIL). OCIL defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions. OCIL may be used in conjunction with other SCAP specifications, such as XCCDF, to help handle cases where lower-level checking languages such as OVAL are unable to automate a particular check. OCIL provides a standardized approach to express and evaluate manual security checks. For example, a system user may be asked, "Do you have a safe to store documents?" The OCIL specification provides the ability to define questions, define possible answers to a question from which the user can choose, define actions to be taken resulting from a user's answer, and to enumerate the result set. One of the benefits of OCIL is that the answers can be returned in a standardized format, allowing statistical analysis and other calculations to be performed in an automated manner.

D.3.2 DATA SOURCES

NIST provides the two data repositories, the NVD and security configuration checklists, to support both automated and manual continuous monitoring efforts.

National Vulnerability Database (NVD)

The NVD is the U.S. government repository of standards-based vulnerability management data represented using the SCAP specifications. This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.

The content in the NVD is dynamic; for example, vulnerabilities are updated with new information such as patch content, checklists are updated, and new checklists are added. As information becomes available in the NVD, systems are rescanned to reassess risk and mitigate any new vulnerabilities. To facilitate a standardized distribution of the data, vulnerability content in the form of XML data feeds is available and updated at two-hour intervals. Organizations can leverage this standardized data for continuous monitoring automation by configuring scheduled scans of systems and evaluating changes that may have occurred and any associated security risks from the changes.

Security Configuration Checklists

The Cyber Security Research and Development Act of 2002[51] tasked NIST to "develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal Government." The National Checklist Program (NCP)[52] is the U.S. government repository of publicly available security checklists. The use of such checklists within the context of an overarching information security program can markedly reduce the vulnerability exposure of an organization.

[51] The Cyber Security Research and Development Act of 2002 is available at http://csrc.nist.gov/drivers/documents/HR3394-final.pdf.

[52] For more information on the NCP, see http://web.nvd.nist.gov/view/ncp/repository.

A security configuration checklist, sometimes referred to as a lockdown guide, hardening guide, or benchmark configuration, is essentially a document that contains instructions or procedures for configuring an information technology (IT) product to a baseline level of security. Checklists can be developed not only by IT vendors, but also by consortia, academia, and industry, federal agencies and other governmental organizations, and others in the public and private sectors.

The NCP provides checklists both in prose format and in SCAP expressed format. The SCAP expressed checklists allow SCAP validated tools to process the checklists and scan systems automatically. A subset of checklists also provides embedded Common Configuration Enumerations (CCEs) mapped to the NIST SP 800-53 security controls that allow for checklist results to be returned in the context of NIST SP 800-53 compliance. A checklist might include any of the following:

- Configuration files that automatically set various security settings (e.g., executables, security templates that modify settings, scripts);
- Documentation (e.g., text file) that guides the checklist user to manually configure software;
- Documents that explain the recommended methods to securely install and configure a device; and
- Policy documents that set forth guidelines for such things as auditing, authentication security (e.g., passwords), and perimeter security.

Not all instructions in a security configuration checklist are for security settings. Checklists can also include administrative practices for an IT product that go hand-in-hand with improvements to the product's security. Often, successful attacks on systems are the direct result of poor administrative practices such as not changing default passwords or failure to apply new patches.

A checklist comparison can also be performed as part of auditing and continuous monitoring of deployed systems' security, to ensure that the baseline configurations are maintained. It is not normally sufficient to configure a computer once and assume that the settings will be maintained; they may change as software is installed, upgraded, and patched, or as computers are connected and disconnected from domains. Users may also alter security settings, such in the case of a user who feels that a locking screen saver is inconvenient and hence turns the feature off.