Supplemental Guidance on Ongoing Authorization

Transitioning to Near Real-Time Risk Management

June 2014

Kelley Dempsey
Ron Ross
Kevin Stine
Computer Security Division
Information Technology Laboratory

National Institute of Standards and Technology
U.S. Department of Commerce

Abstract

Office of Management and Budget (OMB) Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*, stated that, "Our nation's security and economic prosperity depend on ensuring the confidentiality, integrity and availability of Federal information and information systems" and directs the National Institute of Standards and Technology (NIST) to publish guidance establishing a process and criteria for federal agencies to conduct ongoing assessments and authorization. The following additional guidance amplifies current NIST guidance on security authorization and ongoing authorization (OA) contained in Special Publications 800-37, 800-39, 800-53, 800-53A, and 800-137. This guidance does not change current OMB policies or NIST guidance with regard to risk management, information security, security categorization, security control selection, implementation, assessment, continuous monitoring, or security authorization.

Keywords

Federal Information Security Management Act, Information Security Continuous Monitoring, Office of Management and Budget, Risk Management Framework, Ongoing Assessment, Ongoing Authorization.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Additional Information

For additional information on NIST's Computer Security Division programs, projects and publications, visit the Computer Security Resource Center: csrc.nist.gov. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is available at www.nist.gov and www.nist.gov/itl.

NIST Special Publications 800-37, 800-39, and 800-137 are the ***authoritative sources*** on guidance for risk management, authorization/ongoing authorization, and information security continuous monitoring. The guidance in this publication leverages and reinforces the existing guidance and is not intended to diverge from or supersede the guidance in those Special Publications.

Table of Contents

1 Introduction

Office of Management and Budget (OMB) Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*,[1] stated that, "Our nation's security and economic prosperity depend on ensuring the confidentiality, integrity and availability of Federal information and information systems" and directs the National Institute of Standards and Technology (NIST) to publish guidance establishing a process and criteria for federal agencies to conduct ongoing assessments and ongoing authorization.[2] The following additional guidance amplifies current NIST guidance on security authorization and ongoing authorization (OA) contained in Special Publications 800-37, 800-39, 800-53, 800-53A, and 800-137. This guidance does not change current OMB policies or NIST guidance with regard to risk management, information security, security categorization, security control selection, implementation, assessment, continuous monitoring, or security authorization.

2 Background

2.1 Risk Management Framework

NIST developed the Risk Management Framework (RMF) to provide a more flexible, dynamic, approach for effective management of information system-related security risk in highly diverse environments and throughout the system development life cycle. The RMF identifies six steps that provide a disciplined and structured process for managing mission/business risk associated with the operation and use of federal information systems. The six RMF steps include:

- **Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis.
- **Select** an initial set of baseline security controls for the information system based on the security categorization, tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.
- **Implement** the security controls and describe how the controls are employed within the information system and its environment of operation.
- **Assess** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and meeting the security requirements as described in the system security plan.
- **Authorize** information system operation based on a determination of the risk resulting from the operation of the information system, and the decision that this risk is acceptable.
- **Monitor** the security controls in the information system on an ongoing basis, including assessing control effectiveness, documenting changes to the system (or its operating environment), conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Ongoing authorization is part of RMF Step 5, the *Authorize* step, and is dependent on the organization's Information Security Continuous Monitoring (ISCM) strategy and program (summarized in Section 2.3)

---

[1] OMB M-14-03 available at: http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.

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

which is implemented as part of RMF Step 6, the *Monitor* step. OA is fundamentally related to the ongoing *understanding* and ongoing *acceptance* of information security risk. It is also closely related to the dynamic, organization-wide risk management process that develops a more refined and articulated situational awareness of an organization's security and risk posture based on the ongoing assessment, response to, and monitoring of information security risk.

2.2 Security Authorization

Security authorization is the process by which a senior management official, the authorizing official (AO), reviews security-related information describing the current security posture of an information system and uses that information to determine whether or not the mission/business risk of operating a system is acceptable—and if it is, explicitly accepts the risk. The security-related information is presented to the AO either in a security authorization package or by retrieving a report from an automated security management and reporting tool.[3] Security authorization occurs in RMF Step 5, the *Authorize* step.[4] A security authorization can be the initial authorization, ongoing authorization, or a reauthorization as defined below:

- **Initial authorization** is defined as the initial (start-up) risk determination and risk acceptance decision based on a zero-base review of the information system conducted prior to its entering the operations/maintenance phase of the system development life cycle. The zero-base review includes an assessment of *all* security controls (i.e., system-specific, hybrid, and common controls) contained in a security plan and implemented within an information system or the environment in which the system operates.
- **Ongoing authorization** is defined as the subsequent (i.e., follow-on) risk determinations and risk acceptance decisions taken at agreed upon and documented frequencies in accordance with the organization's mission/business requirements and organizational risk tolerance. OA is a time-driven or event-driven security authorization process whereby the AO is provided with the necessary and sufficient information regarding the near real-time security state of the information system (including the effectiveness of the security controls employed within and inherited by the system) to determine whether or not the mission/business risk of continued system operation is acceptable.
- **Reauthorization** is defined as the static, single point-in-time risk determination and risk acceptance decision that occurs after initial authorization. In general, reauthorization actions may be time-driven or event-driven; however, under OA, reauthorization is typically an event-driven action initiated by the AO or directed by the Risk Executive (function) in response to an event that drives information security risk above the previously agreed upon organizational risk tolerance. Reauthorization consists of a review of the information system similar to the review carried out during the initial authorization but conducted *during* the operations/maintenance phase of the system development life cycle rather than prior to that phase. The reauthorization process differs from the initial authorization inasmuch as the AO can initiate: (i) a complete zero-base review of the information system or common controls; or (ii) a targeted review based on the type of event that triggered the reauthorization, the assessment of risk related to the event, the risk response of the organization, and the organizational risk tolerance. Reauthorization is a separate activity from the ongoing authorization process, though security-related information from the organization's ISCM program may still be leveraged to support reauthorization. Note also that reauthorization actions may necessitate a review of and changes to the ISCM strategy which may in turn, affect ongoing authorization.

---

[3] See NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* Appendix D, Section D2, for more information on security management and reporting tools.

[4] For detailed information about security authorization, see NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Chapter 3/Task 5 and Appendix F.

2.3 Information Security Continuous Monitoring

NIST Special Publication 800-137 defines Information Security Continuous Monitoring (ISCM) as maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. An effective ISCM program that is implemented with the appropriate rigor and assessment frequencies to support the organization's mission/business requirements, risk tolerance, and security categorization, is essential to establishing an OA process. Ongoing risk determinations and risk acceptance decisions by senior leaders depend on having relevant and credible near real-time information to help inform such risk determinations and decisions. Special Publication 800-137 defines six steps for achieving effective ISCM:

- **Define** an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission/business impacts.
- **Establish** an ISCM program determining metrics, status monitoring frequencies, control assessment frequencies, and an ISCM technical architecture.
- **Implement** an ISCM program and collect the security-related information required for metrics, assessments, and reporting. 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 ISCM strategy and maturing measurement capabilities to increase visibility into organizational assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization's information infrastructure, and increase organizational resilience.

Ongoing assessment is the continuous evaluation of the effectiveness of security control implementation; it is not separate from ISCM but in fact is a subset of ISCM activities. Ongoing assessment encompasses ISCM Steps 3 and 4 and is initiated as part of ISCM Step 3, *Implement*, when the collection of security-related information begins in accordance with the organization-defined frequencies. Ongoing assessment continues as the security-related information generated as part of ISCM Step 3 is correlated, analyzed, and reported to senior leaders as part of ISCM Step 4. As noted in Special Publication 800-137, security-related information is generated, correlated, analyzed, and reported using automated tools to the extent that it is possible and practical to do so. When it is not possible and practical to use automated tools, security-related information is generated, correlated, analyzed, and reported using manual or procedural methods. In this way, senior leaders are provided with the security-related information necessary to make credible, risk-based decisions regarding information security risk to the mission/business.

3 Ongoing Authorization

3.1 System and Organizational Conditions for Implementation

When the RMF has been effectively applied across the organization *and* the organization has effectively implemented a robust ISCM program, organizational officials, including AOs, are provided with a view of the organizational security and risk posture and each information system's contribution to that security and risk posture on demand. Thus, organizational information systems may move from a static, point-in-time authorization process to a dynamic, near real-time ongoing authorization process when the following conditions are satisfied:

Condition 1 – In accordance with the RMF, the information system has been granted an initial authorization to operate by the AO as a result of a complete, zero-base review of the system[5] and has entered the operations/maintenance phase of the system development life cycle.

Condition 2 – An organizational ISCM program is in place that monitors all implemented security controls with the appropriate degree of rigor and at the appropriate frequencies specified by the organization in accordance with the ISCM strategy and NIST guidance.[6]

The organization defines and implements a process to specifically designate that the system has satisfied the two conditions and has been transitioned to ongoing authorization. This includes the AO formally *acknowledging* that the information system is now being managed by an ongoing authorization process and accepting the responsibility for performing all necessary activities associated with that process. The transition to ongoing authorization is formally documented by the AO by issuing a new *authorization decision document*.[7] The security-related information generated through the continuous monitoring process is typically provided to the AO and other organizational officials in a timely manner through security management and reporting tools. Such tools facilitate risk-based decision making regarding the ongoing authorization to operate for information systems and common controls.

3.2 Information Generation/Collection and Independence Requirements

To support ongoing authorization, security-related information for all implemented security controls, including inherited common controls, is generated and collected at the frequency specified in the organizational ISCM strategy. Security-related information may be collected using automated tools or via other methods of assessment depending on the type and purpose of the security control and the desired degree of rigor. Automated tools may not generate security-related information sufficient to support the AO in making risk determinations because: (i) additional assurance is needed; (ii) the tools do not generate information for every implemented security control or every part of an implemented control; or (iii) the tools do not generate information on specific technologies or platforms. In such cases, manual or procedural security control assessments are conducted at the organizationally-defined frequencies to cover any gaps in automated security-related information generation. The procedurally-generated assessment results are provided to the AO in the manner determined appropriate by the organization.

In order to support OA for moderate-impact and high-impact information systems, the security-related information provided to the AO, whether generated manually/procedurally or in automated fashion, is produced/analyzed by an entity that meets the independence requirements defined by the organization as part of NIST Special Publication 800-53 security control CA-7 (1), *Continuous Monitoring | Independent Assessment*. The independent entity is impartial and free from any perceived or actual conflicts of interest with regard to the development, implementation, assessment, operation, or ongoing management of the organizational information systems and common controls being monitored.[8]

---

[5] As noted in NIST Special Publication 800-37, information system owners and authorizing officials leverage security-related information about inherited common controls from assessments conducted by common control providers.

[6] NIST Special Publication 800-53, security control CA-7, *Continuous Monitoring*; NIST Special Publication 800-53A, which contains information about the appropriate degree of rigor; and NIST Special Publication 800-137.

[7] Most federal agencies have authorization decision documents that include an authorization termination date. By requiring a new authorization decision document, it makes it clear that the information system is no longer bound to the termination date specified in the original authorization document because the agency has now transitioned to OA.

[8] For more information on assessor independence for moderate-impact and high-impact systems, see NIST Special Publication 800-53 security controls CA-2 (1), *Security Assessments | Independent Assessors*, and CA-7 (1), and NIST Special Publication 800-37, Task 4-1, *Develop, Review, and Approve a Plan to Assess the Security Controls.*

3.3 Criteria for Ongoing Authorization and Reauthorization

In NIST Special Publication 800-53, security control CA-6, Part c. requires that the security authorization for an information system and its common (inherited) controls be updated at an organization-defined frequency. This reinforces the concept of ongoing authorization. Thus, in accordance with CA-6 (along with the security control assessment/monitoring frequency determinations defined as part of the ISCM strategy), organizations determine a frequency with which AOs review security-related information via the security management and reporting tool. This near real-time information is used to determine whether the mission/business risk of operating the information system or employing common controls continues to be acceptable. NIST Special Publication 800-137 provides specific criteria for determining appropriate assessment/monitoring frequencies in Section 3.2.2.

Under OA, *time-driven* authorization refers to the frequency with which the organization determines that authorizing officials are to review security-related information and authorize the system (or its common controls) for continued operation as described above. For example, if the organization determines that the frequency for ongoing authorization is weekly for high-impact systems, bi-weekly for moderate-impact systems, and monthly for low-impact systems, AOs would review security-related information for the systems for which they are responsible and accountable to determine ongoing mission/business risk, the acceptability of such risk in accordance with organizational risk tolerance, and whether the approval for continued operation is justified and in the best interest of the organization. The organizational ISCM process, supported by security management and reporting tools, provides the appropriate functionality to notify the responsible/accountable AO that it is time to review the security-related information to support ongoing authorization.

In contrast to time-driven authorization, *event-driven* authorization necessitates an immediate review of security-related information by the AO. Organizations may define event-driven *triggers* (i.e., indicators or prompts that cause an organization to react in some predefined manner) for both ongoing authorization and reauthorization.

- *Ongoing Authorization* – Event-driven triggers for authorization of information systems, common controls, and environments of operation include, but are not limited to, the following:
  - New threat/vulnerability/impact information;
  - An increased number of findings/weaknesses/deficiencies from the ISCM program;
  - New missions/business requirements;
  - A change in the authorizing official;
  - A significant change in risk assessment findings;
  - Significant changes to the information system, common controls, or the environment of operation; or
  - Organizational thresholds being exceeded.

  In such cases, the AO is either notified by organizational personnel (e.g., Chief Information Security Officer, Information System Owner, Common Control Provider, or Information System Security Officer) or via automated tools that defined trigger events have occurred requiring an immediate review of the information system or common controls; or the AO determines (independently) that an immediate review is required. The AO reviews the security-related information via the security management and reporting tool or may request procedurally/manually-generated information in order to make the most effective ongoing risk determinations. This immediate review is *in addition to* the frequency for review defined in the ISCM strategy (i.e., CA-6c./time-driven authorization) as

described above, and occurs within OA when the residual risk remains within acceptable organizational risk tolerance.[9]

- *Reauthorization* – A full reauthorization may be necessary when an event occurs that produces risk above the acceptable organizational risk tolerance (e.g., a catastrophic breach/incident, failure of or significant problems with the ISCM program). The AO or Risk Executive (function) may initiate such a reauthorization as described in Section 2.2 above. Reauthorization actions may necessitate a review of and changes to the ISCM strategy which may in turn affect ongoing authorization.

  Significant changes to an information system or common controls that may trigger an event-driven reauthorization include, but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Significant changes to environments of operation that may trigger an event-driven authorization include, but are not limited to: (i) moving to a new facility; (ii) adding new missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new or modified laws, directives, policies, or regulations.[10] Risk assessment results and/or the results from a security impact analysis may be used to help determine if changes to information systems or common controls are significant enough to trigger a reauthorization action.

Finally, in accordance with OMB Memorandum 14-04, OA fulfills the three-year security reauthorization requirement required by OMB Circular A-130. The following excerpts from the OMB memorandum state the federal policy regarding ongoing authorization and supporting ISCM programs.

34. Is a security reauthorization still required every 3 years or when an information system has undergone significant change as stated in OMB Circular A-130?

No. Rather than enforcing a static, three-year reauthorization process, agencies are expected to make ongoing authorization decisions for information systems by leveraging security-related information gathered through the implementation of ISCM programs. The implementation of ISCM and ongoing authorization thus fulfill the three-year security reauthorization requirement, so a separate re-authorization process is not necessary.* In an effort to implement a more dynamic, risk-based security authorization process, agencies should follow the guidance in NIST Special Publication 800-37. Agencies will be required to report the security state of their information systems and results of their ongoing authorizations through CyberScope in accordance with the data feeds defined by DHS.

* The transition from the three-year reauthorization approach to ongoing authorization should be carried out in accordance with the level of maturity and effectiveness of agency ISCM programs, organizational risk tolerance, and subject to the final decision of authorizing officials.

[9] The *immediate* reviews initiated by specific trigger events may occur simultaneously (i.e., in conjunction) with time-driven monitoring activities based on the monitoring frequencies established by the organization and how the reviews are structured within the organization. The same reporting structure may be used for both types of reviews to achieve efficiencies.

[10] The examples of changes listed above are only *significant* when they meet the threshold established in the definition of significant change (i.e., a change that is likely to affect the security state of the information system). Organizations establish such definitions of significant change based on a variety of factors including for example: mission/business needs; threat and vulnerability information; environments of operation for information systems; and security categorization.

35. How can my agency use ISCM to inform ongoing authorization decisions?

Agencies should develop and implement ISCM strategies for all information systems which address all security controls implemented, including the frequency and degree of rigor associated with the monitoring process. ISCM strategies should also include all common controls inherited by organizational information systems. ISCM strategies should be developed in accordance with NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, and approved by appropriate authorizing officials. Agency officials should monitor the security state of their information systems on an ongoing basis with a frequency sufficient to make ongoing risk-based decisions on whether to continue to operate the systems within their organizations.

ISCM programs and strategies should address: (i) establishment of metrics to be monitored; (ii) establishment of frequencies for monitoring/assessments; (iii) ongoing security control assessments to determine the effectiveness of deployed security controls; (iv) ongoing security status monitoring; (v) correlation and analysis of security-related information generated by assessments and monitoring; (vi) response actions to address the results of the analysis; and (vii) reporting the security status of the organization and information system to senior management officials consistent with guidance in NIST SP 800-137.

3.4 The Process: RMF Step 5, Authorize

The following section: (i) reiterates the specific tasks in RMF Step 5 (i.e., security authorization of the information system or common controls); and (ii) provides amplifying guidance on any OA-specific issues related to those authorization tasks.

TASK 5-1: Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.

Under OA, other than specific weaknesses or deficiencies (or defects) being identified from the output of the ISCM program in near real-time, the Plan of Action and Milestones (POA&M) process is unchanged from that defined in NIST Special Publication 800-37. The information to be included in the POA&M and an organizational strategy to facilitate a prioritized approach to risk response is described in Task 5-1 Supplemental Guidance.

TASK 5-2: Assemble the security authorization package and submit the package to the authorizing official for adjudication.

Under OA, the AO requires information from the System Security Plan (SSP), the Security Assessment Report (SAR), and the POA&M in order to make ongoing risk determinations/risk acceptance decisions. To support ongoing authorization and to provide information to the AO in the most efficient and timely manner possible, the security authorization package, consisting of the SSP, the SAR, and the POA&M, is presented to the AO via automated reports.[11] Information to be presented in the SAR is generated using the near-real time security-related information from the ISCM program and presented to the AO in a report using an organization-selected automated security management and reporting tool, the format and frequency of which is determined by the organization (see Section 3.3 above). The SAR information presented to the AO includes security-related information about *all* implemented system-specific, hybrid,

[11] While the objective is to fully automate all components of the security authorization package including the SSP, SAR, and POA&M, organizations may be in various states of transition to such a fully automated state—that is, with certain sections of the authorization package available via automated means and other sections available only through procedural/manual means.

and common controls. Similarly, the AO uses the automated security management and reporting tool and/or other automated methods to access the SSP and the POA&M which are kept in current status in accordance with near real-time risk management objectives using automated and/or manual update processes as determined by the organization. While the initial data *entry* for the SSP, SAR, and POA&M may be automated, procedural/manual, or both, in order to support ongoing authorization and near real-time risk management objectives in general, it is important that security-related information be accessible to the AO in an automated fashion.[12]

TASK 5-3: Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

Under OA, the process for determination of risk by the AO is unchanged from that defined in NIST Special Publication 800-37. The AO assesses the security-related information provided by the automated security management and reporting tool regarding the current security state of the system and inherited common controls and the recommendations for addressing residual risks in accordance with the risk management strategy (including organizational risk tolerance).

TASK 5-4: Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.

Under OA, the process for acceptance of risk by the AO is unchanged from that defined in NIST Special Publication 800-37. The AO continues to be responsible and accountable to explicitly *understand* and *accept* the risk of continuing to operate the system. However, under OA, the authorization termination date may not be specifically stated; rather, the organization defines in its continuous monitoring strategy, the appropriate frequency, level of effort, and event triggers that inform the generation of information needed to make ongoing risk determinations and risk acceptance decisions. Therefore, in lieu of an authorization decision document that specifies an authorization termination date, the AO affirms or withholds agreement for continued operation of the information system (or the organization-defined common controls). In other words, instead of specifying an authorization termination date, the AO reviews the security-related information with the frequency defined by the organization as part of the ISCM strategy (see Section 3.3 above) and either acknowledges that the risk of continued system operation or use of the common controls remains acceptable, or indicates that the risk is no longer acceptable and requires further risk response.

The organization determines the level of formality required for the acknowledgement by the authorizing official. The AO may continue to convey terms and conditions to be followed by the information system owner or common control provider for continued authorization to operate. The terms and conditions may be conveyed, at the discretion of the organization, through the automated security management and reporting tool (i.e., creating an automated authorization decision document). The AO may also use the tool to annotate Risk Executive (function) input. As stated in Task 5-4 Supplemental Guidance in NIST Special Publication 800-37, organizations may eliminate the authorization termination date *only* if the ISCM program is sufficiently robust to provide the AO with the near real-time information needed to support ongoing risk determinations and ongoing risk acceptance decisions.

[12] Organizations decide on the level of granularity and presentation format of security-related information that is made available to the AO through automation. These decisions are based on the needs of the organization with the automated presentation of security-related information tailored to the decision-making needs of the AO. For example, very detailed security-related information may be generated and collected at the operational level of the organization with such information subsequently analyzed, distilled, and presented to the AO in a summarized or highlighted format using automation.

3.5 Transitioning from Static Authorization to Ongoing Authorization

The intent of ISCM is to monitor security controls with the frequency needed to provide AOs with the necessary and sufficient information to make effective, risk-based decisions, whether by automated or procedural/manual means. However, if a substantial portion of monitoring is not ultimately accomplished via automation, it will not be feasible or practical for organizations to move from the current static authorization approach to an effective and efficient ongoing authorization approach. A phased approach for the generation of security-related information may be necessary in the interim as additional automated tools become available and a greater number of security controls are monitored by automated techniques. Organizations may begin by generating security-related information from automated tools that are in place and fill in gaps by generating additional security-related information from procedural/manual assessments. As additional automated monitoring functionality is added, processes can be adjusted.

Transitioning from a static authorization process to a dynamic, ongoing authorization process requires considerable thought and preparation. One methodology that organizations may consider is to take a phased approach to the migration based on the security categorization of the system. Because risk tolerance levels for low-impact systems are likely to be greater than for moderate-impact or high-impact systems, implementing ISCM and OA for low-impact systems first may help ease the transition and allow organizations to incorporate lessons learned as ISCM and OA are implemented for moderate-impact and high-impact systems. This will facilitate the continued steady and consistent progression of the ISCM and OA implementation from the lowest to the highest impact levels for the systems within the organization. Organizations may also consider employing the phased implementation approach by partitioning their information systems into well-defined subsystems or system components and subsequently transitioning those subsystems and/or system components to OA one segment at a time until the entire system is ready for the full transition (at which time the AO acknowledges that the system is now being managed by an ongoing authorization process).

4 Conclusion

While it is dependent on a robust ISCM program, implementation of ongoing authorization within an organization does *not* change the security authorization process as defined in NIST Special Publication 800-37 in any fundamental way—rather, it makes the process more efficient and produces more timely information for AOs to support risk-based decision making with regard to the information systems and common controls supporting organizational missions/business functions. AOs continue to review security-related information and either grant authorization to operate by explicitly understanding and accepting the risk of operating information systems (or implementing common controls) or alternatively, deny authorization to operate because the risk is determined to be unacceptable. Organizations simply leverage the security-related information generated as part of the comprehensive ISCM program to provide AOs with near real-time, security-related information about the security status/risk posture of information systems or common controls for which they are responsible and accountable. Organizations determine the frequency with which the AOs review such information in order to make informed risk determinations—and ultimately decide if the mission and/or business risk is acceptable as part of an organization's careful consideration of risk tolerance.

5 References

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 14-03, *Enhancing the Security of Federal Information and Information Systems*, November 2013.
3. Office of Management and Budget Memorandum 14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 2013.
4. 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.
5. National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.
6. National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013.
7. National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010.
8. National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011.