Creating More Effective – and Strategic – Solutions


Erik Ebel
William Gulley
July 2014

Ongoing Authorization – What is it and how has it changed?

Most can agree that quite a bit has changed in the world of cybersecurity since the White House and the Office of Management and Budget (OMB) released Circular No. A-130. This memorandum established the first recommended frequency at which federal departments and agencies would review security controls for system security authorization decisions: “when significant modifications are made to the system, but at least every three years.” Conceived almost fifteen years ago, this model and review cycle was developed to address the pace at which vulnerabilities emerged and threats evolved at that point in time.

As more data, commerce, and processes shifted towards models that utilize information systems to conduct business, the industry’s exposure to more vulnerabilities and a greater number of threat vectors elicited the need to reconsider the overall security authorization process. The need for “continuous” or more frequent reviews of the overall system security posture and supporting security controls grew each subsequent year after A-130 was released. Figure 1 below illustrates the evolution of system security authorization processes and the development of continuous monitoring concepts to validate that federal systems are operating at acceptable levels of risk.

As the graphic above indicates, a more proactive approach was developed to test security controls in subsets over the course of the maximum three year authorization period. New supporting processes such as Continuous Monitoring and Information Security Continuous Monitoring (ISCM) (in more recent years) have rapidly evolved as support mechanisms to the system security authorization process.

The concept of Ongoing Authorization (OA) is much more than testing controls more frequently than the previously established “once every three years” approach. In June 2014, the National Institute of Standards and Technology (NIST) released guidance entitled Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management as it relates to the
rapidly increasing utilization of ISCM as an integral supporting process. The guidance defines Ongoing Authorization 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.” The guidance goes on to further delineate the difference from legacy security authorization processes to Ongoing Authorization as a, “time-driven or event-driven security authorization process whereby the Approving Authority 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.” The process and frequency at which to review and authorize risk levels as outlined in the guidance yields the ability to more effectively assess and authorize system risk levels on an ongoing and near real-time basis.

What is the marriage between OA and ISCM?

When the NIST and Department of Homeland Security (DHS) conceived ISCM, and Continuous Diagnostics and Mitigation (CDM), respectively, the security control assessment data collection conduit to support an Ongoing Authorization model was successfully established. The new Ongoing Authorization guidance set forth by NIST outlines the relationship and dependency between ISCM/CDM assessment data and the future ability to measure the security posture of a given information system in a near real-time fashion. One of the benefits that ISCM provides is the near real-time collection of “actual state” data from production environment systems in a given organization. This ISCM actual state data collection is compared to the expected, desired state for a specific “check” or “test,” which can often be mapped back to a NIST 800-53 control, and provides the foundation for the Ongoing Assessment portion of Ongoing Authorization. This single test or assessment case ultimately replaces the traditional manual control tests performed under legacy security authorization processes.

For example, the Manage Vulnerabilities CDM capability includes a number of defect checks that can be mapped to a specific 800-53 control in many instances. If a single defect check (test case) yields actual state data that does not match the expected, desired state for that defect check when the supporting CDM tool performs the test, some level of risk is determined. The aforementioned process performs similar to the way our legacy security authorization processes would determine some level of risk when a control failed a test during the system security authorization process (where the legacy process involves an individual or individuals subjectively qualifying a risk level). As one can see, the automated handling of controls testing (via ISCM/CDM tools) significantly reduces the time spent performing security authorization activities and increases situational awareness levels relative to security posture for authorization decisions.

What is the criteria to get started?

The new NIST guidance states that Ongoing Authorization of a system can take place when two conditions are met:

Condition 1 – In accordance with the Risk Management Framework (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 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.

The first condition is the more simplistic of the two requirements. An organization planning to adopt Ongoing Authorization to replace legacy security authorization processes for a system must ensure that the system has been initially accredited/authorized utilizing legacy security authorization processes. First, the Authorizing Authority must accept the level of operational risk present in the system. Once the system moves to the production environment, the organization can begin the transition to Ongoing Authorization.

Independent of the design, implementation, and maintenance of the organization’s ISCM/CDM solution, the second condition requires the greater amount of effort to achieve. To the greatest extent feasible, the organization should seek to align or map the defect checks/tests performed under the auspices of the organization’s CDM/ISCM program (for each ISCM/CDM capability as outlined below in Figure 2) to the applicable security controls from NIST 800-53 and any other organization-specific controls that are required from a compliance standpoint.
Once the organization and the Approving Authority come to an agreement on the satisfaction of the security control mapping to the ISCM/CDM defect checks (tests), the foundational exercise will be complete. Most entities will find that a portion of their controls may not map to the ISCM/CDM defect checks. The testing and assessment of these controls will likely retain their legacy processes for validation of effectiveness. This notion will not prevent an organization from completing their migration to Ongoing Authorization; these controls will simply be tested at lesser frequency than those that are part of the automated Ongoing Assessment process. Ultimately, the reduction of manual testing will significantly reduce the effort required to conduct the security authorization process, and yields a level of risk situational awareness relative to a system in near real-time that was not previously possible.
References


http://www.whitehouse.gov/omb/circulars_a130_a130trans4


http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf


