What Continuous Monitoring Really Means

By Ron Ross

National Institute of Standards and Technology

Recently, NIST completed a fundamental transformation of the traditional certification and accreditation process into a comprehensive, near real-time, security life cycle process as part of a Risk Management Framework (RMF). The RMF, described in NIST Special Publication 800-37, provides a dynamic, six-step approach to managing cybersecurity risk. The strength of the RMF is based on the comprehensive nature of the framework which focuses as much attention on selecting the right security controls and effectively implementing those controls as it does on security assessment, authorization, and continuous monitoring. The strategy is simple. "Build It Right, Then Continuously Monitor." The RMF, when used in conjunction with the three-tiered enterprise risk management approach described in NIST SP 800-39 (Tier 1-governance level, Tier 2-mission/business process level, and Tier 3-information system level) and the broad-based continuous monitoring guidance in NIST SP 800-137, provides a comprehensive process for developing, implementing, and monitoring a cybersecurity program capable of protecting core organizational missions and business functions from a range of threats, including cyber attacks.

There are some significant problems that can arise if organizations move down the continuous monitoring road with a narrow focus on security controls at the information system level without first doing some basic investment in strengthening their underlying information technology (IT) infrastructure. First, organizations may end up wasting significant resources monitoring inherently weak information systems—in essence, throwing good money after bad. You can check that broken lock on the front door of your house once a day or every hour, and the lock is still broken. Better to fix the lock first, reinforce the door jamb, and then with the remaining resources, check the lock on an ongoing basis. Second, premature allocation of resources toward continuous monitoring of security controls at Tier 3 may preclude organizations from investing the resources needed to build stronger, more penetration-resistant information systems—systems that are better prepared to address the advanced persistent threat and the cyber attacks that are associated with highly sophisticated and well-resourced adversaries. This is especially important for information systems that support the U.S. critical infrastructure, including for example, power generation and distribution facilities, financial institutions, transportation modalities, and the defense industrial base.

Strengthening the IT infrastructure begins with establishing a sound cybersecurity and risk management governance process at Tier 1. Next, at Tier 2, organizations must manage the complexity of their IT infrastructures by using enterprise architecture to consolidate, standardize, and optimize the current inventory of IT assets as well as developing "threat aware" mission and business processes. Organizations must also develop and integrate into their enterprise architecture, a security architecture that guides the effective and efficient allocation of needed security controls to their information systems at Tier 3. And finally, organizations must initiate continuous monitoring of all of the above activities to ensure ongoing effectiveness of cybersecurity and risk management governance, mission/business processes, enterprise and security architectures, and security controls deployed within the enterprise.

To summarize, failure to deploy available continuous monitoring resources in the right sequence and with the right level of effort could have significant potential adverse effects on the national and economic security interests of the United States. Continuous monitoring will be most effective when applied across all key components of an organization—from governance to architecture to systems. Continuous monitoring, broadly applied, can provide important benefits to organizations with regard to cybersecurity and risk management. It can support and enhance a dedicated, mature process for building the necessary trustworthiness into the information systems that are supporting the nation's most important missions and business functions both in the public and private sectors.