Establishing a **Secure** Framework

CONTINUOUS MONITORING is an important part of an agency's cybersecurity efforts. But without establishing an effective security framework first, those efforts may be misspent.

The National Institute of Standards and Technology recently completed a fundamental transformation of the certification and accreditation process into a comprehensive, near real-time security lifecycle process as part of a Risk Management Framework (RMF).

The RMF 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 them 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 a three-tiered enterprise risk management approach and broad-based continuous monitoring, provides a comprehensive process for developing, implementing and monitoring a cybersecurity program. Such a program can protect core organizational missions and business functions from a range of threats, including cyberattacks.

CRITICAL NIST SECURITY GUIDANCE

NIST offers comprehensive guidance on information security and continuous monitoring:

- **NIST Special Publication 800-37**
  Guide for Applying the Risk Management Framework to Federal Information Systems
- **NIST SP 800-39**
  Managing Information Security Risk
- **NIST SP 800-137**
  Information Security Continuous Monitoring for Federal Information Systems and Organizations

Build a Foundation First

Organizations that begin work on a continuous monitoring program with a narrow focus on security controls at the information system level without first doing some basic investment in strengthening their underlying IT infrastructure face significant problems.

First, they may end up wasting significant resources monitoring inherently weak information systems — in essence, throwing good money after bad. You can check a broken lock on the front door of your house once a day or every hour, but the lock is still broken. Better to fix the lock first, reinforce the doorjamb, and then with the remaining resources, check the lock on an ongoing basis.

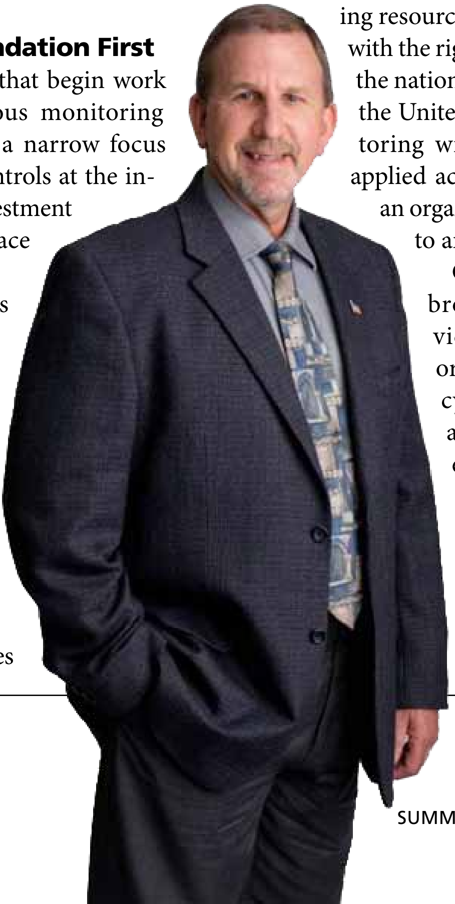
Second, premature allocation of resources toward continuous monitoring of security controls for information systems may preclude organizations from investing the resources needed to build stronger, more penetration-resistant systems. Such investments are critical as agencies address the advanced persistent threat and cyberattacks associated with sophisticated and well-resourced adversaries. This is especially important for information systems that support critical infrastructure.

Strengthening the IT infrastructure begins with establishing a sound cybersecurity and risk management governance process. Next, 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 allocation of security controls to their information systems. 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.

Failure to deploy continuous monitoring resources in the right sequence and with the right level of effort could harm the national and economic security 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. FT


JAMES KEGLEY

Dr. Ron Ross is a Fellow with the National Institute of Standards and Technology.