Assessing Security Controls

Keystone of the Risk Management Framework

CISOs and CSOs need to ensure that their enterprise risk management programs have a solid foundation—the enterprise risk management framework. This framework should provide a disciplined and structured process that integrates risk management activities into the system development life cycle and enables risk executives to make informed decisions. The US National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) is such a framework. Commitment to a risk management framework and robust risk principles are critical for a successful risk management program.

Making informed risk decisions involves risk-decision fidelity and steps to determine risk acceptance. A good recipe for making risk decisions includes a mixture of:

- Objective data
- Pass/fail test results
- Mitigations
- Qualitative analysis
- Subjective data
- A healthy portion of intuition

The subjective data may raise eyebrows. This ingredient considers probability and questions who provides the data, as the data source could be important. The intuition portion is also not as objective as facts such as test results. Intuition does not lend itself to a quantitative risk model, rather, qualitative analysis is a key ingredient in the decision-making recipe.

Practitioners inherit a variety of risk management programs in various states over their careers. Some are actually quite good, some are adequate and others are complete disasters. Regardless of the state of the program, sticking to a framework and solid risk principles is critical.

During the last five years, the NIST RMF has gained extensive use across the United States and several other nations. NIST developed and published the elements that an enterprise needs to implement and manage a robust risk management program. The NIST RMF includes the system development life cycle phases and the steps that risk management organizations should follow (**figure 1**).

Test, Test, Test

Although all of the steps of the NIST RMF are important, Step 4: Assess Security Controls is the most critical step of a risk management program. Testing the system thoroughly and then performing ruthless configuration management to maintain the security are essential. If the system is tested properly, it will be fundamentally secure. If the enterprise maintains a secure system configuration, the system basically stays at the same level of security. Often, enterprises do not adequately test systems, and the mechanisms to verify accurate auditing of security assessments and other controls are lacking. Nothing can substitute for assessing security controls. Some of the reasons for this lack of security controls assessment are:

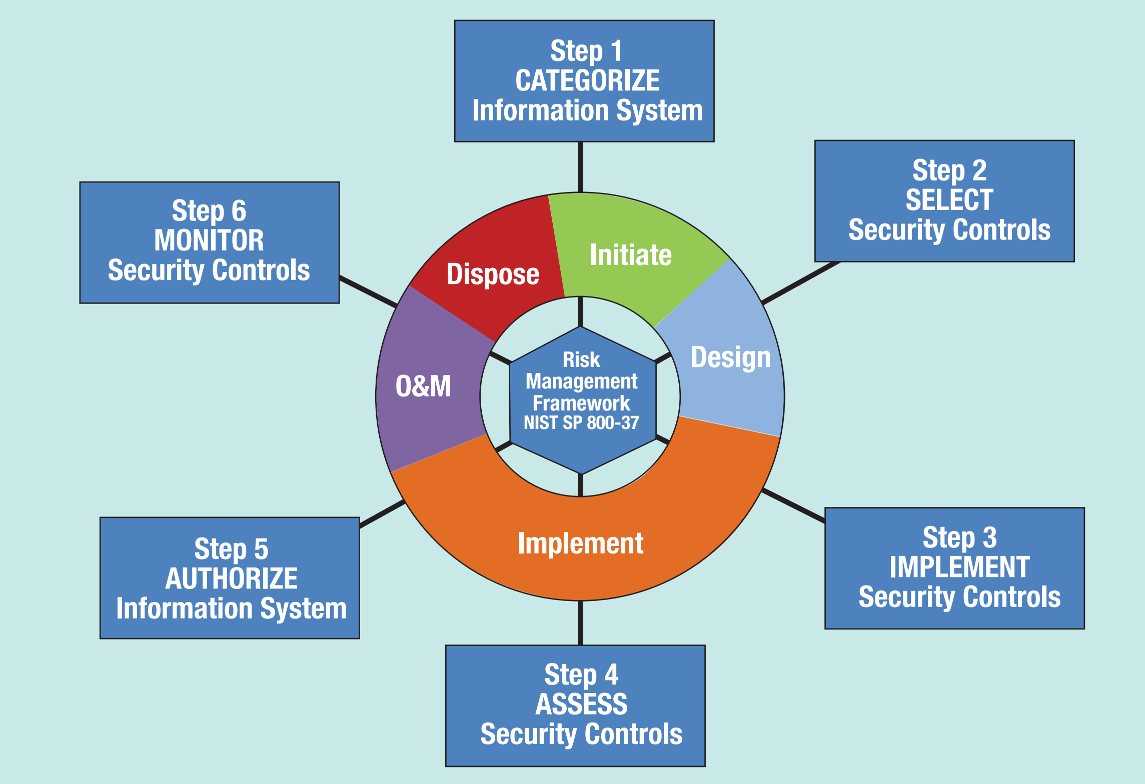
- Leadership not providing clear expectations for assessing controls/testing schedules
- Inadequate oversight of the risk management program
- Lack of skilled test managers and testers/security assessors
- Leadership pressure to condense the testing cycle due to the schedule having a higher priority than the security of a system

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® web site *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Lance Dubsky, CISM, CISSP
Is chief security strategist, global government, at FireEye and has more than two decades of experience planning, building and implementing large information security programs. Before joining FireEye, he served as the chief information security officer for two US intelligence agencies, where he led global security programs. In the realm of risk management, Dubsky has served as a senior risk executive, authorizing official, certification official and security control assessor. He managed the transformation to the US NIST Risk Management Framework at two organizations, optimized risk processes by merging risk and system development life cycles, and established a risk assessment process for satellite platforms.

Figure 1—NIST Risk Management Framework



Source: National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems,* NIST Special Publication 800-37, Revision 1, February 2010, figure 2-2. Reprinted with permission.

How testing is audited is also a challenge for enterprises implementing a risk management program. Quality assurance or compliance oversight is often underfunded or lacks the experience to identify the red flags.

The Basic Security Assessment Process

In NIST RMF Step 4: Assess Security Controls, NIST guidelines recommend testing all of the applicable security controls in NIST Special Publication 800-53[1] for which the system has been categorized. The only way to know whether a security control works or not, or passes or fails, is to test it. Testing security controls cannot be achieved through a vulnerability scanning tool, which only checks a small number of security controls. A vulnerability scan often tests a fraction, approximately five percent, of the security controls.

> **“The only way to know whether a security control works or not, or passes or fails, is to test it.”**

The role of the security assessor/tester is to test all key security controls for a system and account for all of the security controls for which the system was categorized in step 1 of the NIST RMF. The role may also include the development and execution of the test plan for the system. The test plan includes all controls for which the system has been categorized. The security assessor executes the test plan with the system owner and records the results. The results of the NIST RMF step 4, which is also referred to as the security assessment phase, include:

- A list of applicable security controls
- A test plan encompassing all of the applicable security controls
- A test report (pass/fail)
- Mitigations for any failed controls

These results are the outcome of a basic security assessment process and provide the risk executive with the information that is required to make a risk decision. Within the US intelligence community, the risk executive is designated by the agency director and is often the chief information officer (CIO), deputy CIO, chief information security officer (CISO) or director of risk management; however, enterprises may designate the risk executive in a different way.

If an enterprise security assessment process does not have this level of integrity and fidelity, risk decisions are being made basically without the necessary information. A great risk management program follows the security assessment process and performs penetration testing after the system is risk accepted and in operation. However, as a risk executive, the most important, the most revealing and the most objective step of the risk management framework is the assessment of security controls. If this risk management phase is not performed correctly, the ability to legitimately accept the risk is virtually impossible.

What Is an Auditor to Do?

Each year, the public sector submits metrics and measures in support of government compliance and reporting requirements. Some of these many metrics include:

- The number of systems that the enterprise operates
- The number of enterprise systems that have an authorization to operate
- The number of enterprise systems that have risk acceptance

The fidelity of measuring the effectiveness of a risk management program rests in whether the security controls are being tested and retested periodically, and whether a record of test results exists.

In the US intelligence community, many auditors and compliance officers, as a normal course of their duties, perform an annual audit of the agency's risk management program and processes to validate whether the program is being run according to standards and to validate the accuracy of the metrics that are being reported. The auditors use a relatively small team, sometimes a third party, to perform the audit. The auditor reviews a subset of the agency systems, because most agencies have hundreds to thousands of systems. Some of the subsets are a small .001 percent of the total number of agency systems. This method does not reveal the true state of the agency risk management program and whether the steps of the RMF, especially testing, are being performed. Too few systems are reviewed and the review is often time consuming.

Audit teams should pivot and focus on a broader set of systems and a more detailed review of the integrity of testing. To broaden the set of systems, the teams will have to be less in-depth on the

overall review of the system and focus on the most revealing step of the RMF—the available evidence to determine the integrity of step 4. If the organization has 1,000 systems, the organization should have 1,000 test plans and the test results for each system. The exception would be if the systems use centralized security services available from the enterprise. If audit teams can determine the existence of system test plans and test results and interview the security assessors, the teams can accurately determine whether the system was tested completely and whether the risk executive has the most objective data to make a risk decision. If the system is not tested or inadequately tested, the risk acceptance or authorization to operate should be invalidated.

> **“If the system is not tested or inadequately tested, the risk acceptance or authorization to operate should be invalidated.”**

Enterprise leadership needs to set expectations for the enterprise risk management program and how the program will be measured, especially the security assessment phase of the risk management framework. For auditors, asking the right questions is crucial to discovering the true state of how the risk management program is working and the integrity of the program. The following specific requests can reveal a great deal to an audit team, to a CISO and to the CIO:

- Archive of test plans for each system, with test result, per system. A test plan will have all security controls for which the system was categorized.
- How many of the security controls were tested manually? Who performed the test?
- How many of the controls were tested with a tool or application? Which tools were used and what specific controls did each tool test?
- Of the total number of security controls, how many passed?
- Of the total number of security controls, how many failed? What were the compensating mitigations? Was the mitigation tested?
- Where is this system physically set in the enterprise and to what is it connected?
- Does the system security documentation reflect all of the above?

If an enterprise uses the NIST RMF and the risk management program can successfully answer the questions for each of its systems, the foundation of the risk management program is solid. No program is perfect; however, if an enterprise is assessing security controls with a high degree of fidelity and the auditor can verify this fidelity, then the enterprise risk management program is in good, if not great, shape.

Endnotes

[1] National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4, USA, April 2013, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*