The PCI DSS and the NIST and ISO Risk Assessment Protocols

There is some justifiable confusion about how the PCI DSS and the requirements for risk assessment under DSS 12.1 interact. Quoting from the September 2006 DSS update,

"12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:

12.1.1 Addresses all requirements in this specification

12.1.2 Includes an annual process that identifies threats and vulnerabilities, ***and results in a formal risk assessment***

12.1.3 Includes a review at least once a year and updates when the environment changes."

The two most common formal risk assessments for information security are from the International Standards Organization or ISO and from the National Institute for Standards and Technology or NIST. Risk assessment software is available for both procedures from various vendors, including PCI SVA members ACR2 (NIST) and Modulo (ISO).

The NIST framework includes ALL of the minimum standards required of US Federal agencies. This is a longer list than the PCI "digital dozen" and includes some items that may not be applicable to all PCI organizations. However, the NIST framework provides an inexpensive way to obtain a "formal risk assessment" that is traceable to an objective outside standard. The ISO framework is even longer, making the NIST a little easier to use.

Every PCI DSS standard is included in the NIST listing, along with some additional risk related items such as maintenance procedures and contingency planning which are somewhat neglected by the DSS.

It is important to realize that just because an element is not specified in detail in the DSS does not mean that it does not affect both the risks to cardholder information and the results of the risk assessment. An example of this expansion is section 2.2 of the DSS as quoted below.

"2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS)."

The PCI specification calls out SANS, NIST and CIS configuration standards **in addition to** the digital dozen and incorporates them by reference.

To a large extent, the PCI DSS standard is more granular and has more specific details in the items it does include than the NIST listing. For example, very specific details are given in DSS

section 3 about handling procedures for Primary Account Numbers (PAN). On the other hand, the NIST provides copious details for a variety of options by cross-referencing the NIST protocols with 92 volumes of backup documentation. This can be particularly useful when organizations are attempting to use compensating controls under Appendix B of the DSS.

To summarize, there are a lot of options for creating a formal risk assessment. At present, the simplest and least expensive option is to use one of the existing risk assessment software programs, either ISO or NIST, and take advantage of the continuous updating provided by these sponsoring organizations.