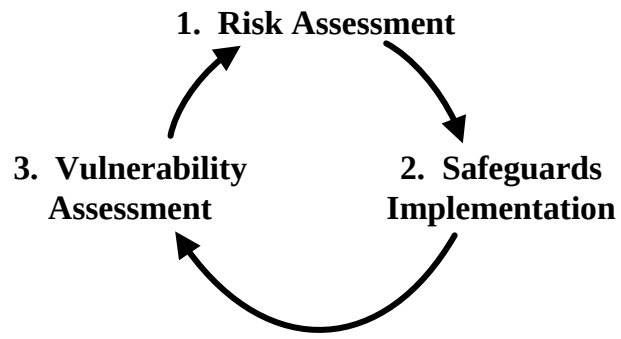
Closing the Circle of Compliance: SCAP, XCCDF, OVAL and ACR2

Information security is one of the great vulnerabilities of modern civilization. In 2004 cybercrime exceeded illegal drugs as the leading criminal enterprise (1). Now in 2007 this problem has spawned a wide variety of regulations and technologies to deal with information security issues.

The general form of an information security compliance program is similar across a large number of regulatory frameworks, including the Gramm Leach Bliley Act (GLBA), the Payment Card Industry Digital Security Standard (PCI DSS), the Federal Information Security Management Act (FISMA) and the Health Insurance Portability and Accountability Act (HIPAA). In each case a risk assessment (step 1) is followed by implementation of safeguards (step 2) to meet the risks identified and quantified in step 1. The implementation of safeguards is followed by vulnerability testing (step 3) of the safeguards implemented in step 2. The results of the vulnerability testing are incorporated into a revised risk assessment and the cycle continues. This "Circle of Compliance" process is shown graphically below.



Risk assessment is a difficult and unfamiliar process and a wide variety of risk assessment formats have been proposed. Under FISMA, Federal agencies are required to use the risk assessment protocols developed by the National Institute of Standards and Technology (NIST). HIPAA and GLBA regulators recommend these standards as well. The NIST protocols also meet the PCI DSS requirement for a "formal risk assessment" and are compatible with the ISO 27001 framework.

The first NIST computer security standards were published in 1985 as the Special Publications 500 series. In 1996 under the Clinger-Cohen Act, the NIST was tasked with setting minimum standards for computer security for Federal agencies. Annual audits of compliance with these standards are done by the Office of the Inspector General. These standards are currently published by the NIST as the Special Publications 800 Series (2).

The NIST standards for risk assessment and computer security have many advantages for organizations regulated under such statutes as HIPAA and GLBA. Since the regulators have to comply with the same standards, both sides of the table are familiar with the same approach (3). Meeting the same standards as a Federal agency allows regulated organizations to state that they have met or exceeded "appropriate" precautions against "reasonably foreseeable" risks (GLBA).

The disadvantages of the NIST standards are also significant. The standards are lengthy and complicated; with many of them written at an 18th grade Flesch-Kincaid reading level. This makes them difficult to use for persons without advanced academic degrees.

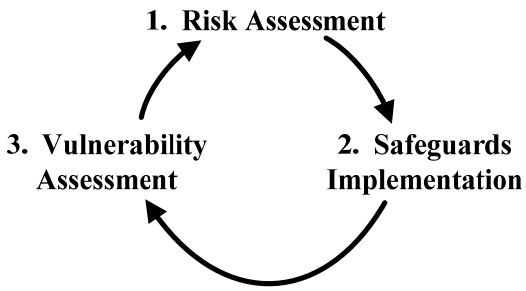
An almost complete set of the NIST protocols involving risk assessment, as of March 2007, is shown in the photo at the right.

Following the NIST standards for such requirements as audits (4), intrusion detection (5) logs and vulnerability testing (6) generates very large amounts of data that are difficult to analyze. Regulations such as the GLBA require even very small organizations, such as community banks, to comply with security standards that they are unprepared to meet.

One potential answer to this dilemma is automation. At present, four key programs involved in information security automation are the Security Content Automation Protocol (SCAP), the Open Vulnerability and Assessment Language (OVAL) initiative, the Extensible Configuration Checklist Description Format (XCCDF) protocol and the Automated Compliance Reporting 2 program (ACR2).

SCAP is an interagency program involving OSD, DHS, NSA, DISA, and NIST. OVAL and XCCDF, jointly published by the NIST and NSA, are both protocols under SCAP. OVAL is supported by an international organization funded by the US Office of Homeland Security. ACR2 is an automated repackaging of the NIST risk assessment protocols, similar to the "Turbo-Tax™" software widely used for US income tax compliance.

All of these programs are evolving very rapidly. The XCCDF was issued in April of 2007, with the first SCAP release of tools for Windows™ systems issued May 22, 2007. OVAL 5.2 was released in January 2007, while version 5.3 is scheduled for release in June of 2007. ACR2 was released in November 2006 and the first OVAL compatible version is scheduled for July 2007.



In the Circle of Compliance, SCAP, OVAL and XCCDF are focused on steps 2 and 3, safeguards implementation and vulnerability assessment. ACR2 is directed at step 1, risk assessment.

Commercial organizations are following the government lead. The Payment Card Industry Security Vendors Alliance (PCI SVA) is an organization of approximately 70 vendors of security solutions to the 20 million organizations regulated under the PCI DSS. It has been recommended that the SVA Solutions Committee consider the OVAL output specification as a uniform recommendation to its members. Some SVA members such as ConfigureSoft are in compliance with OVAL (7) while others such as ACR2 have already scheduled OVAL compliance for at least some of their products in the very near future.

There is no magic bullet for information security compliance. However, automation programs such as ACR2, SCAP and OVAL can do a lot to close the Circle of Compliance.

www.acr2solutions.com Phone: 404-372-2820 Fax: 770-381-9229 Email: robert.p@acr2solutions.com