Automation Support for FISMA Compliance – Automating Compliance with the Certification and Accreditation Requirements of the Federal Information Security Management Act and OMB Circular A-130

Information security is a major issue for federal networks. Despite years of effort and billions of dollars of expense, most federal networks get marginal grades for FISMA compliance. In May 2008 it was announced that federal systems averaged a grade of "C", up slightly from C- the year before. Although some agencies are doing well, departments, commissions and agencies with graded "F" in 2007 included the Transportation Department, the Labor Department, the Defense Department, the Interior Department, the Treasury Department, the Nuclear Regulatory Commission, the Veterans Affairs Department and the Agriculture Department.

In response to these problems, ACR 2 Solutions has combined network scanning from the DHS Security Content Automation Program (SCAP) with automated NIST 800-30 risk assessment protocols to provide a powerful new tool to automate large portions of the FISMA Certification and Accreditation (C&A) process. The automated risk management process reduces the time required for risk assessment by 70-90%, freeing up scarce technical manpower to work on remediation rather than documentation.

FISMA Requirements

The FISMA requirements are contained in Public Law No: 107-347 and summarized below;

§ 3544. Federal agency responsibilities
(a) IN GENERAL.—The head of each agency shall...
(2) ensure that senior agency officials provide information security ... through—
(A) **assessing the risk** [emphasis added]
(B) determining the...information security [that is] appropriate
(C) implementing policies and procedures...
(D) periodically testing...security controls

A FISMA amendment bill , with expected changes coming in 2010, would significantly expand FISMA requirements to include outside audits, annual DHS reports and require that poorly secured networks be cut off from the federal system.

Risk Based Certification and Accreditation.

The NIST protocol on C&A, 800-37, is strongly focused on risk based prioritization of activities. Quoting from page 1, " *It is essential that agency officials have the most complete, accurate, and trustworthy information… in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems.* Unfortunately, manual risk assessment using the 800-30 protocol is a long and resource intensive process. A partial copy of the references involved in an 800-30 risk assessment is shown at right.

The FISMA Compliance Reporter automates the risk assessment process using artificial intelligence tools taken from the process control industry. The automated process was validated using manual assessments from consultants in the financial area, and the results have been audited by both the OCC and the FDIC. A detailed description of the risk assessment automation process is available on the references page of the compliance support website, www.compliance.acr2solutions.com.

Automating Risk Management – NIST 800-37 and the DHS SCAP Program

Details on the Risk Management Framework (RMF) process are found in Special Publication 800-37 from the National Institute of Standards and Technology (NIST). At present, the federal RMF process consists of four steps; Initiation Phase, Security Certification, Security Accreditation and Continuous Monitoring. The current draft revision of 800-37 raises the bar significantly, calling for "near real-time risk management". The revised NIST 800-37 will apply to both civilian and defense agencies, and is designed to provide a "common foundation for information security for all federal agencies and contractors" (NIST 800-37, rev 1, page vii).

Within the last 12 months powerful new tools have been developed for information security under the DHS Security Content Automation Protocol (SCAP) program. The first network scanner to be SCAP validated, C5, is now available from Fortinet Federal, along with the FortiGate NIAP certified Intrusion Prevention Systems. SCAP scanning, IPS and AV data and policy data combine to form the Automated FISMA Compliance Process.

Automated FISMA Compliance Process

The Compliance Reporter process is straightforward.

1. Determine the FIPS 199 classification of the network, low, medium or high.
2. Scan the network using an SCAP validated scanner. Upload the scan results.
3. Upload the network intrusion and virus data from the previous week, month or quarter.
4. Fill out the Risk Reporter questionnaire.
5. Request an 800-30 Risk Assessment Report.

A baseline report from Compliance Reporter is shown at right.

Symbol	Threat Source	Vulnerability	Likelihood	Impact	Baseline Score
E1	Wind	Roof damage	M	H	H
E2	Fire	Smoke damage	M	H	H
E3	Flood	Facility damage	M	H	H
E4	Power loss	Loss of operations	M	H	H
E5	Power loss	Damage to building	M	H	H
E6	Vehicle collision	Facility damage	M	H	H
HE1	Human error	Data acquisition	M	H	H
HE2	Human error	Data storage	M	H	H
HE3	Human error	Data retrieval	M	H	H
HE4	Human error	Data modification	M	H	H
HE5	Human error	Data transmission	M	H	H
HE6	Human error	System design	M	L	L
HE7	Human error	Procedure implementation	M	H	H
HE8	Human error	Internal controls	M	H	H
MI1	Malicious insider	Data acquisition	M	M	M
MI2	Malicious insider	Data storage	M	M	M
MI3	Malicious insider	Data retrieval	M	M	M
MI4	Malicious insider	Data modification	M	M	M
MI5	Malicious insider	Data transmission	M	M	M
MI6	Malicious insider	System design	M	L	L
MI7	Malicious insider	Procedure implementation	M	H	H
MI8	Malicious insider	Internal controls	M	H	H
MO1	Malicious outsider	Data acquisition	M	L	L
MO2	Malicious outsider	Data storage	M	L	L
MO3	Malicious outsider	Data retrieval	M	L	L
MO4	Malicious outsider	Data modification	M	L	L
MO5	Malicious outsider	Data transmission	M	L	L
MO6	Malicious outsider	System design	M	L	L
MO7	Malicious outsider	Procedure implementation	M	L	L
MO8	Malicious outsider	Internal controls	M	L	L

Compliance Reporter Support for FISMA Requirements

The Compliance Reporter supports a variety of FISMA C&A process elements, as defined by NIST 800-37.

Initiation Phase - Initial network scan and equipment inventory, Initial inventory of security controls, Initial assessment of risk using the NIST 800-30 protocol.
Security Certification Phase - Confirm and document status of security controls, Revised risk assessment, Initial risk based Plan of Action and Milestones (POAM)
Continuous Monitoring Phase - Periodic network scanning and configuration monitoring, Auto-updating of 33 security controls, Security impact analysis and updated risk assessment, POAM updating and status reports.

Additional Information and Onsite Demonstrations.

For more information on the FISMA Compliance Reporter, email info@acr2solutions.com, call Robert Deitz at 800-326-5683 or visit the website, www.compliance.acr2solutions.com. FISMA Compliance software is sold on the GSA Schedule 70 by ACR Partner GV Technologies.