ACR 2 Solutions, Inc.

Automated Risk Management Using NIST Standards

The management of risks to the security and availability of protected information is a key element of privacy legislation under the Federal Information Security Management Act (FISMA), the Gramm Leach Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS). In the case of FISMA, the information security responsibilities of agency heads are summarized as follows:

> H. R. 2458
> § 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

Similar language is present in the other privacy legislations. In each case, the process begins with risk assessment, and then moves on to management of the assessed risks.

Technical risk assessment is a relatively recent art that grew out of the environmental remediation industry in the 1980s. It was not until 2002 that the National Institute of Standards and Technology (NIST) produced a protocol detailing risk assessment for information security, although it was alluded to in earlier documents.

Since the Clinger-Cohen Act of 1996, the National Institute of Standards and Technology has been required to set the standards for information security. The publication of the risk assessment procedure NIST 800-30 in 2002 both eased and complicated the burden on organizations required to complete risk assessments. Although it established the procedure for assessing risk, the standards are both voluminous and complex. Conducting a NIST compliant risk assessment remains problematic for many organizations. A single copy of the applicable NIST references as of mid-2007 is shown at right.

The documentation of 800-30, while detailed, is well written. On page 8, the protocol states that "The risk assessment methodology encompasses nine primary steps…

Step 1 System Characterization (Section 3.1)
Step 2 Threat Identification (Section 3.2)
Step 3 Vulnerability Identification (Section 3.3)
Step 4 Control Analysis (Section 3.4)

Step 5 Likelihood Determination (Section 3.5)
Step 6 Impact Analysis (Section 3.6)
Step 7 Risk Determination (Section 3.7)
Step 8 Control Recommendations (Section 3.8)
Step 9 Results Documentation (Section 3.9)."

1. System Characterization (3.1)

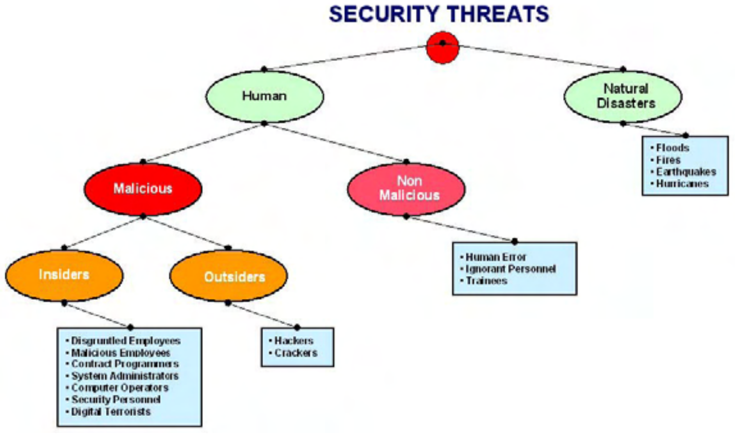
Page 12 of 800-30 requires questionnaires, document review, and automated scanning tools for system characterization. The Security Content Automation Program (SCAP), started in 2005, calls for the use of SCAP validated scanners to confirm continued compliance with security guidelines.

The Automated Risk Management program from ACR utilizes a variety of SCAP validated scanners. In addition, an extensive policy questionnaire is also used, keyed to the appropriate NIST requirements taken from NIST 800-53. SCAP scanners can report NIST 800-53 compliance status for a large number of network devices and workstations, and compliance checklists are under development for additional platforms.

2. Threat Identification (3.2)

Page 13 of 800-30 lists natural threats, human threats, and environmental threats. An early 2001 information security paper by Jaisingh and Rees refers to the Microsoft classification of threats as being divided into Natural Disasters, Human Error, Malicious Insiders and Malicious Outsiders. Later papers, by Mintaka (2003) and Altoros (2007), include a more elaborate version of the Rees diagram.

While there are other acceptable ways to identify threats, the dominance of Microsoft products in the Federal space indicates that the use of the Microsoft division of threats into Environmental, Human Error, Malicious Insiders and Malicious Outsiders is both useful and widely acceptable. The Rees diagram is shown below.



3. Vulnerability Sources (3.3)

In 2005, the NIST created the National Vulnerability Database (NVD), which superseded the I-CAT database referred to on page 16 of 800-30. The NVD is incorporated into the SCAP validated scanner that is part of the Automated Risk Management program from ACR.

Page 18 of 800-30 notes that vulnerabilities in management, operational, and technical areas all need to be considered.

The Automated Risk Management program from ACR system further divides vulnerable areas into management (Procedure implementation and Internal controls), operational (Data acquisition, Data storage, Data retrieval, Data modification, Data transmission) and technical (System design). In addition, the environmental vulnerabilities of Wind (roof damage), Fire (and smoke) damage, Flood, Power loss (loss of operations), Power loss (Damage to building), and Vehicle collision are included. It is believed that this division was taken from an early risk assessment draft, but the original source has been lost.

Other division of areas of vulnerability could be made, but these are reasonably comprehensive and are easily assigned to particular 800-53 safeguards.

4. Control analysis (3.4)

The utility of the 800-30 process was greatly enhanced by the 2005 publication of 800-53, “Recommended Security Controls for Federal Systems.” For the first time, a listing of adequate safeguards to achieve an acceptable level of risk was made explicit by an authoritative source.

This frequently updated list, in conjunction with the SCAP validated scan engine, is the basis for much of the Automated Risk Management program from ACR process.

Two key elements in control analysis are anti-virus protection and intrusion protection. Both are highly important precautions, and the volume of virus and intrusion traffic is closely associated with the current security level of a network. A badly infected network will be both compromised and slow, as more and more network resources are misapplied by unauthorized uses. Typically a Unified Threat Management (UTM) appliance will be used to provide this information.

5. Likelihood determination (3.5)

For an 800-30 risk assessment, likelihood has a specific legal meaning, as follows;

> *High* - The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.

Medium - The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

Low - The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Since the publication of 800-30 in 2002, cybercrime has rivaled illegal drugs as the leading criminal activity worldwide. Threat source motivation and capability can reasonably be assumed.

The Automated Risk Management program from ACR utilizes the safeguards of NIST 800-30. Mapping of these safeguards to the four threat sources (Environmental, Human Error, Malicious Insider and Malicious Outsider) is done by inspection. For each threat source, the vulnerable areas of management (Procedure implementation and Internal controls), operations (Data acquisition, Data storage, Data retrieval, Data modification, Data transmission), and technology (System Design) are also fairly obvious although extensive. The overall mapping exceeds 5,000 entries.

The validation of the safeguards map into an expert system computer program was done by observing experienced risk assessment consultants and tweaking the calculation engine to produce the same results using either a human expert or the expert system computer program. This makes the program useful, but risk assessment using this procedure, or any procedure, has limited precision and granularity. As noted in 800-39, the “flagship document” of the NIST 800 series, “Managing risk is not an exact science”.

Information security risk assessments produced with this system have been audited by both OCC and FDIC experts.

6. Impact analysis (3.6)

Impact levels under 800-30 have very specific definitions.

High - Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human death or serious injury.

Medium - Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human injury.

Low - Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization’s mission, reputation, or interest.

The calculation of impact levels is also mapped to 800-53 safeguards in a fairly obvious fashion. For example, a system that does not meet the requirements of safeguard CP-9, Information System Backup, will be much more impacted by Fire than a system which is compliant with CP-9 and has a well written contingency plan (CP-2) that includes training (CP-3) and testing (CP-4).

7. Risk determination (3.7)

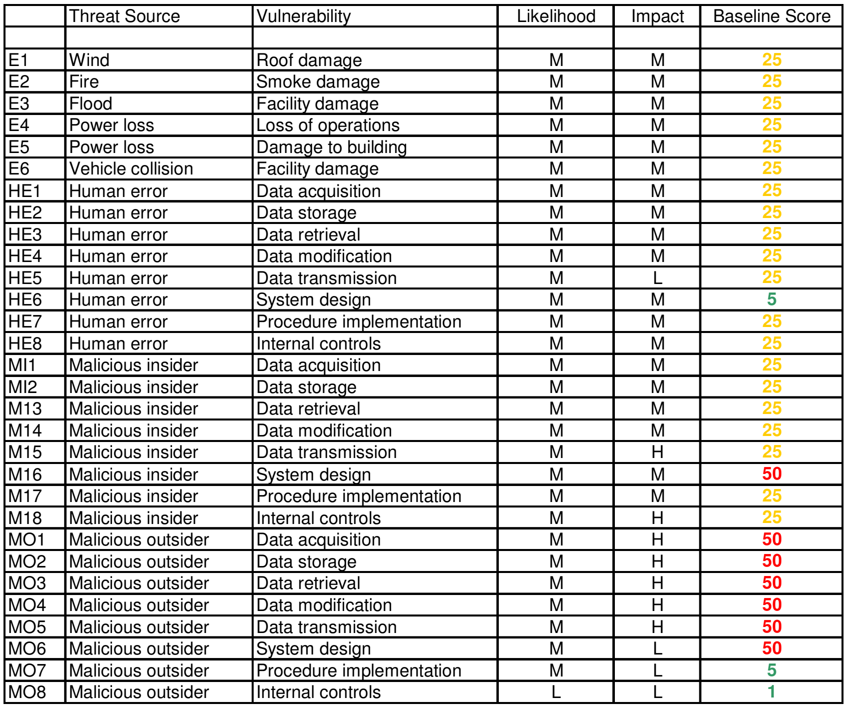
The calculation algorithm for the risk assessment is given on page 25 of 800-30. Low, Medium, and High likelihoods of adverse events are scored at 0.1, 0.5 or 1.0, respectively. In the same manner, Low, Medium, and High impacts are scored at 10, 50 and 100 respectively. By multiplying the likelihood score and the impact score, a risk score from 1 (low) to 100 (high) is calculated.

8. Control recommendation (3.8)

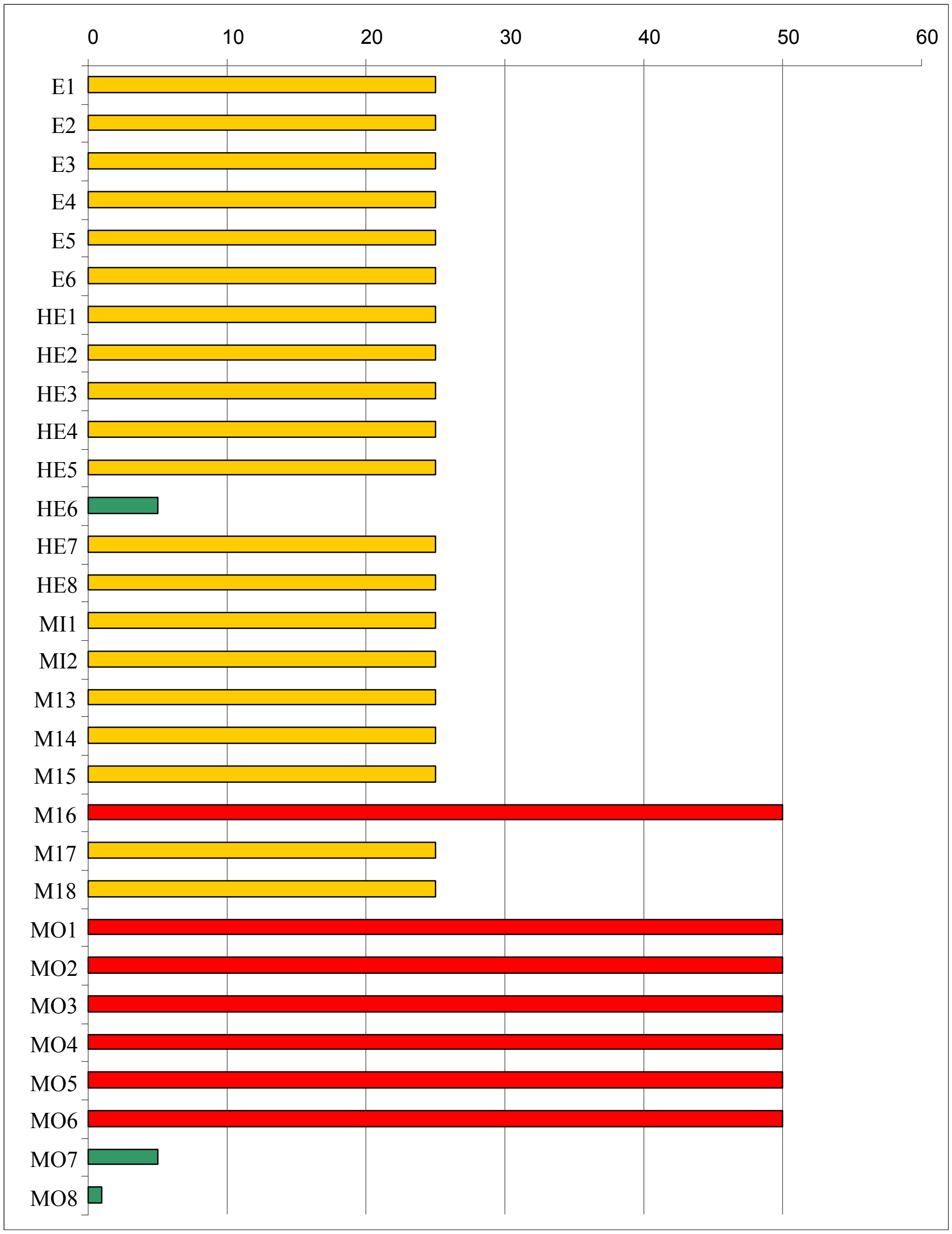
These reports give a mapping of the featured safeguards which are missing, against the identified risks in order of impact. These reports should be used to determine which safeguards need to be changed or updated.

9. Results documentation

Upon completion of the Automated Risk Management program from ACR risk assessment, the initial set of data will produce two reports, a "Baseline Report" showing the risk scores ordered by threat source and a "Risk Assessment Chart." with the same risk scores shown in graphical form. A sample is shown below.



	Threat Source	Vulnerability	Likelihood	Impact	Baseline Score
E1	Wind	Roof damage	M	M	25
E2	Fire	Smoke damage	M	M	25
E3	Flood	Facility damage	M	M	25
E4	Power loss	Loss of operations	M	M	25
E5	Power loss	Damage to building	M	M	25
E6	Vehicle collision	Facility damage	M	M	25
HE1	Human error	Data acquisition	M	M	25
HE2	Human error	Data storage	M	M	25
HE3	Human error	Data retrieval	M	M	25
HE4	Human error	Data modification	M	M	25
HE5	Human error	Data transmission	M	L	25
HE6	Human error	System design	M	M	5
HE7	Human error	Procedure implementation	M	M	25
HE8	Human error	Internal controls	M	M	25
MI1	Malicious insider	Data acquisition	M	M	25
MI2	Malicious insider	Data storage	M	M	25
M13	Malicious insider	Data retrieval	M	M	25
M14	Malicious insider	Data modification	M	M	25
M15	Malicious insider	Data transmission	M	H	25
M16	Malicious insider	System design	M	M	50
M17	Malicious insider	Procedure implementation	M	M	25
M18	Malicious insider	Internal controls	M	H	25
MO1	Malicious outsider	Data acquisition	M	H	50
MO2	Malicious outsider	Data storage	M	H	50
MO3	Malicious outsider	Data retrieval	M	H	50
MO4	Malicious outsider	Data modification	M	H	50
MO5	Malicious outsider	Data transmission	M	H	50
MO6	Malicious outsider	System design	M	L	50
MO7	Malicious outsider	Procedure implementation	M	L	5
MO8	Malicious outsider	Internal controls	L	L	1



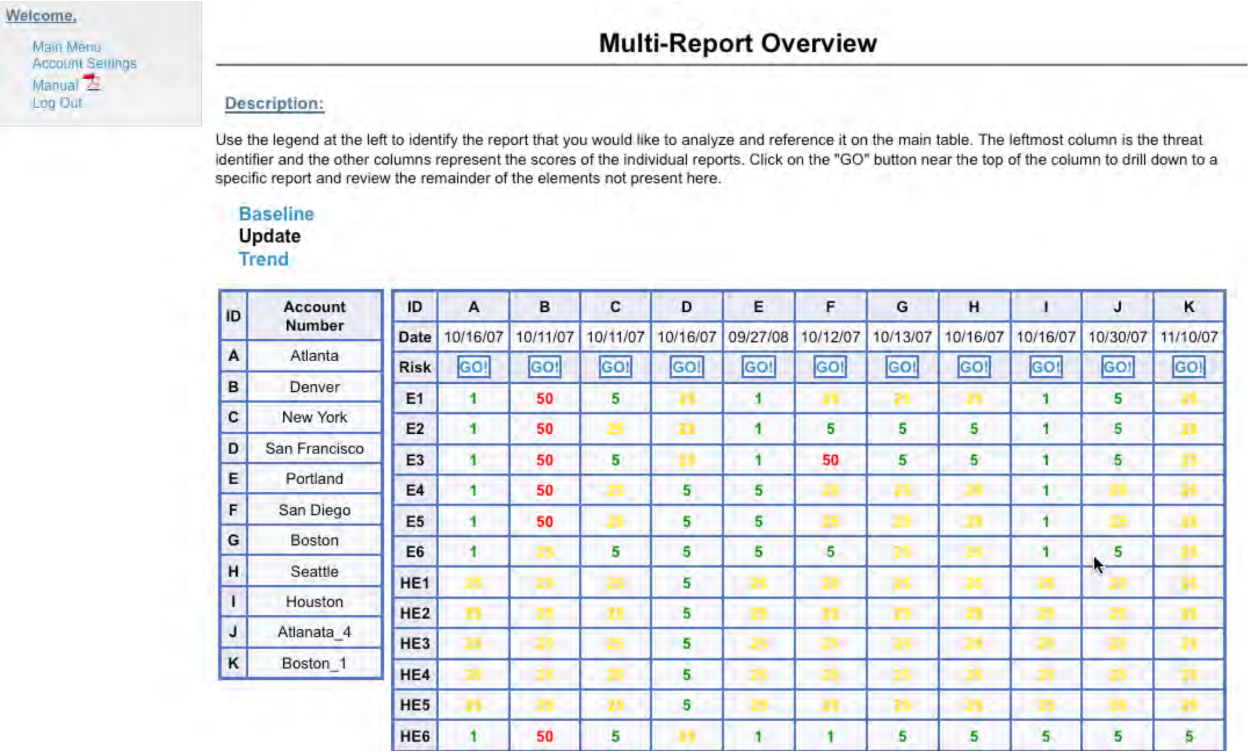
An annual NIST 800-30 compliant risk assessment is required under several sets of regulations, but is likely to be far outside the experience of most security officers who do not have extensive risk assessment experience. The burden these regulations place on organizations can be eased by the use of Automated Risk Management program from ACR. This regulatory burden will only be increased by the adoption of NIST 800-39. The new "flagship document" in the FISMA compliance series requires "near real-time" management and assessment of risk. While there is not yet an official definition of "near real-time" it is likely to be far more often than annually.

The ACR automated risk management process can cycle as often as daily, which is probably as close to “near real-time” as is practical given the normal variability in intrusion detection data. Daily automated updating of UTM and SCAP scan data on a university network was demonstrated for six months in 2008 at Clarkson University. This level of “near real-time” risk management is expected to become the standard of care in the near future.

The typical bank customer for ACR updates risk assessments monthly in preparation for Board of Directors meetings. Under the Gramm Leach Bliley Act (GLBA), bank directors are personally liable for penalties up to $12,000 per day of non-compliance with information security requirements. FISMA regulated networks are typically updated quarterly, as are HIPAA regulated networks.

Managing Multiple Networks

The same process used for single network risk management can also be applied to groups of networks. The Enterprise version of the ACR software, shown below, can group network status summaries onto a single display console.



Multi-Report Overview

Description:

Use the legend at the left to identify the report that you would like to analyze and reference it on the main table. The leftmost column is the threat identifier and the other columns represent the scores of the individual reports. Click on the "GO" button near the top of the column to drill down to a specific report and review the remainder of the elements not present here.

ID	Account Number
A	Atlanta
B	Denver
C	New York
D	San Francisco
E	Portland
F	San Diego
G	Boston
H	Seattle
I	Houston
J	Atlanata_4
K	Boston_1

ID	A	B	C	D	E	F	G	H	I	J	K
Date	10/16/07	10/11/07	10/11/07	10/16/07	09/27/08	10/12/07	10/13/07	10/16/07	10/16/07	10/30/07	11/10/07
Risk	GO!	GO!	GO!	GO!	GO!	GO!	GO!	GO!	GO!	GO!	GO!
E1	1	50	5	25	1	25	25	25	1	5	25
E2	1	50	25	25	1	5	5	5	1	5	25
E3	1	50	5	25	1	50	5	5	1	5	25
E4	1	50	25	5	5	25	25	25	1	25	25
E5	1	50	25	5	5	25	25	25	1	25	25
E6	1	25	5	5	5	5	25	25	1	5	25
HE1	25	25	25	5	25	25	25	25	25	25	25
HE2	25	25	25	5	25	25	25	25	25	25	25
HE3	25	25	25	5	25	25	25	25	25	25	25
HE4	25	25	25	5	25	25	25	25	25	25	25
HE5	25	25	25	5	25	25	25	25	25	25	25
HE6	1	50	5	25	1	1	5	5	5	5	5

The Enterprise group management process is particularly useful for organizations that are required to assess the risk involved in passing protected information to other users. For example, hospitals under HIPAA are now required to assess the security status of business associates to whom they send Protected Health Information (PHI).

Under the 2009 American Recovery and Reinvestment Act (ARRA) business associates of HIPAA covered entities are directly responsible for HIPAA Security Rule compliance, and potential fines have been increased from $25,000 to $1,500,000. This dramatically increases the potential liability for hospitals that transmit protected information to insecure associates.

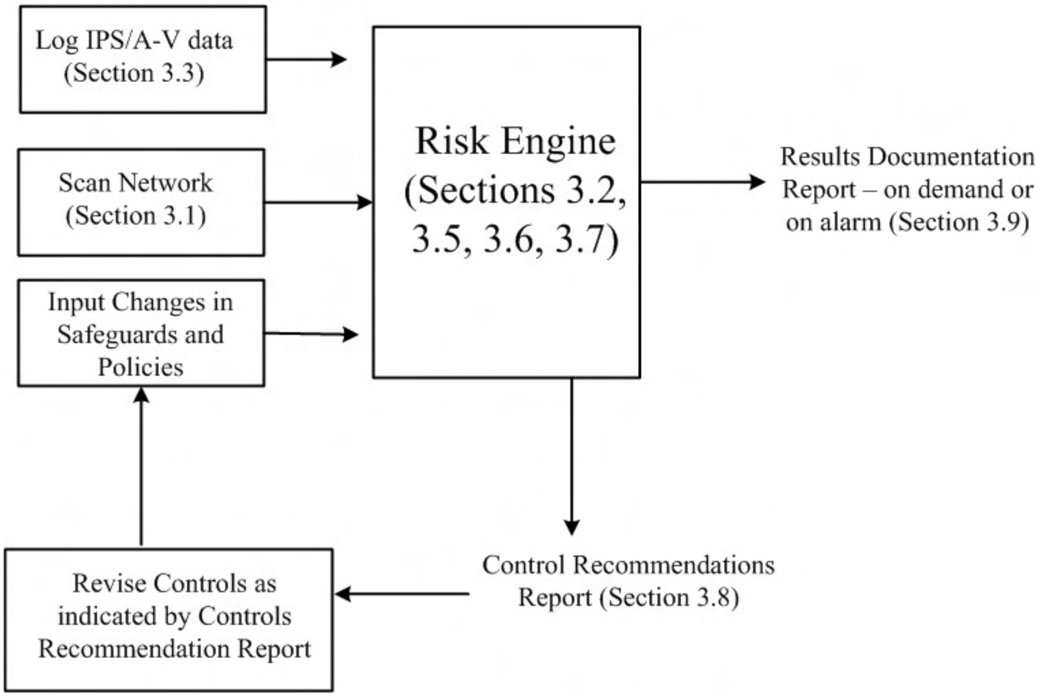
In December of 2009 the ACR Enterprise software was installed in a series of four New York hospitals. The CIO of the lead hospital, Massena Memorial, stated that "…we are requiring all affiliated business associates of the hospital to use the ACR 2 Solutions software…". A copy of this endorsement letter is available on the ACR website at www.acr2solutions.com.

Megaprise Edition

A Megaprise version of the ACR Risk Management software is also available to manage groups of network groups. The Megaprise Edition can provide single console risk management for a mixture of single network and Enterprise Edition network groups. The number of networks that can be managed is a function of server size, and is readily expandable.

Overall Risk Management Process

The overall risk management process is shown below in graphical form. Data from a network scan (800-30 section 3.1), IPS and AntiVirus data (Section 3.3) and policy data are input into the Risk Engine. This creates Results Documentation (Section 3.9) and recommendations for change.

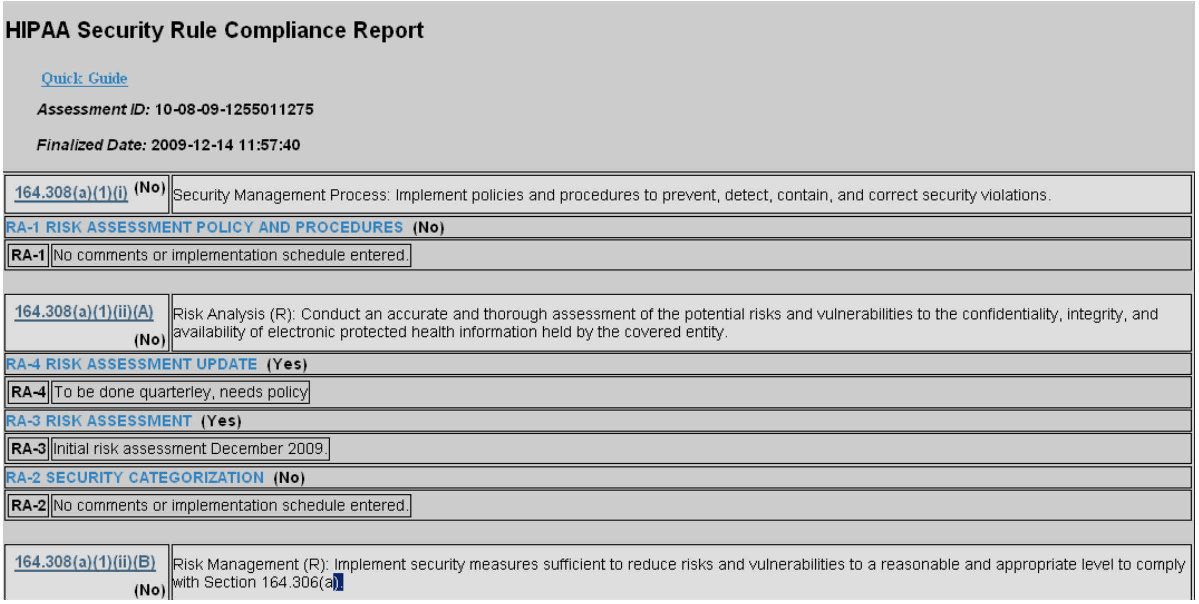

Log IPS/A-V data (Section 3.3)
Scan Network (Section 3.1)
Input Changes in Safeguards and Policies
Risk Engine (Sections 3.2, 3.5, 3.6, 3.7)
Results Documentation Report – on demand or on alarm (Section 3.9)
Control Recommendations Report (Section 3.8)
Revise Controls as indicated by Controls Recommendation Report

The changes in Controls are implemented and the changes added to the risk engine, along with updated Scan and IPS/A-V data. This cycle can be easily done as often as daily, with reports on demand, on schedule, or on alarm. Reports on alarm can be emailed to an administrator or used to create a text message for transmission to a phone. A patent application has been filed covering this process.

Fully Integrated Automated Risk Management Programs

The integrated NIST 800-30 programs combine IPS, A-V, scanning and risk assessment data to meet the complete needs of a risk management program. There are four versions of this program currently available, covering report templates under HIPAA, GLBA, PCI and FISMA regulations. Each of these regulatory schemes can utilize the 800-30 risk assessment methodology, but their downstream reporting requirements differ. For example, the NIST 800-66 requirements under HIPAA are a subset of the NIST 800-53 requirements under FISMA.

The data used to create the risk assessments can be reused to create other required reports. For example, a 45 CFR Part 164 compliance report (see below) can be generated using the risk assessment information and the associated NIST crosswalk. Similarly, FISMA NIST 800-37 C&A reports can be created using the risk assessment information.



HIPAA Security Rule Compliance Report

Quick Guide

Assessment ID: 10-08-09-1255011275

Finalized Date: 2009-12-14 11:57:40

164.308(a)(1)(i) (No) Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES (No)

RA-1 No comments or implementation schedule entered.

164.308(a)(1)(ii)(A) (No) Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

RA-4 RISK ASSESSMENT UPDATE (Yes)

RA-4 To be done quarterley, needs policy

RA-3 RISK ASSESSMENT (Yes)

RA-3 Initial risk assessment December 2009.

RA-2 SECURITY CATEGORIZATION (No)

RA-2 No comments or implementation schedule entered.

164.308(a)(1)(ii)(B) (No) Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

Automated Near Real-Time Risk Management

Information security risk management has become so complex that only automation makes it possible to enjoy a reasonable degree of information security. The ACR integrated risk management programs can help deal with the ever-increasing threats to information security. The NIST protocols define “appropriate safeguards” for information security. The ACR automation of the NIST protocols makes the appropriate safeguards usable and affordable, and provides the “near real-time” management of risk that is the goal of the SCAP program.