Using ACR 2 Reports

Creating Compliance Action Plans

After entering and reviewing system data on information security, users will receive either a baseline or an update set of reports depending on whether information is entered for the first time in a fiscal year - the baseline report set, or as an update to the initial status – the update report set. Depending on the version of ACR2 Basic you have purchased, users are allowed to update their risk assessments as often as weekly, although a monthly update is most common. Either set of data will generate four encrypted .pdf reports (copies in Risk Assessment folder on this CD):

1. Baseline.pdf or Update.pdf - a numerical scoring of risks to information security and availability. Risks, defined as threat source/vulnerability combinations, are divided into 30 risk categories based on NIST protocols. Risks range from E1, wind/roof damage to MO8, malicious outsider/internal controls. A full listing of risk categories is found at the end of this document.

2. Chart.pdf - a graphical, color coded representation of the baseline or update risk scores. Red/yellow/green coding indicates high, medium and low risk status, respectively.

3. Status.pdf - a compilation of the current status of the safeguards for this information system compared to the minimum recommended standards for Federally regulated networks under NIST protocols.

4. Deficiency.pdf - a cross listing of missing or underperforming safeguards with risk categories for this system at this time.

Following review and acceptance of these risk reports by Management, it is necessary to create an action plan to prioritize and upgrade system safeguards to continue to comply with information security regulations. Compliance under GLBA, HIPAA or PCI is a continuously moving target. Regulated firms are required to;

1. Assess risks
2. Install safeguards
3. Test safeguard performance
4. Re-assess risks

This is an ongoing cycle that will continue as long as the organization remains in operation.

Prioritizing your activities

The ACR2 reports are designed to efficiently prioritize and organize the updating and upgrading of information security safeguard to produce an action plan. According to NIST standards, risks scoring > 50 need to be immediately addressed, risks scoring from 10 to 50 need to be scheduled

for management, and risks <10 can be monitored without further action. These risk levels are graphed at red, yellow and green, respectively in the chart.pdf report.

Creating a safeguard action plan

To create a safeguards action plan, review the chart.pdf report and/or the baseline/update report. On a separate page, list the risks by category, ie red, yellow, green. For the chart sample below, the red scored risks are MO7 and MO8, the green are E2 and E3, HE 6&7 and MI 6, while the other risks score into the yellow range.

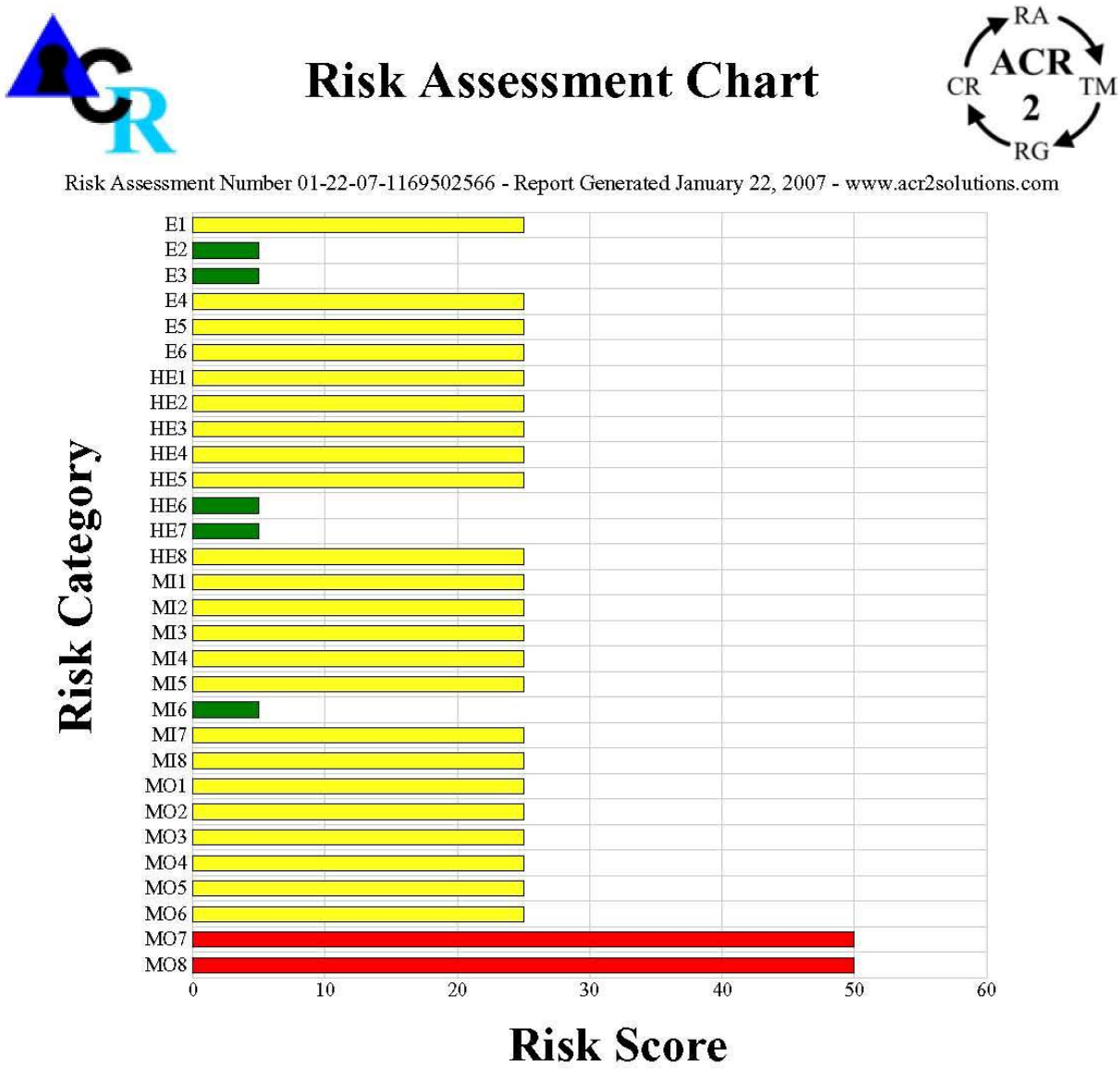

Table A1: Risk Assessment Chart

Using the associated Deficiency Report (Table A2), list the missing or underperforming safeguards associated with the red scored risks, in this case MO7 and MO8. In this case, the safeguards that affected the red risks are the same and include:
AC-11, -13. -17, -18, AU-3, CA-1, CP-2, -8, IA-1, -4, IR-3, Ma-5, PL-3, -4, PS-7, RA-5, SA-6, -9, SC-4, -7, SI-2 and SI-5.

Once the needed safeguards are identified, they can be listed using data from the Deficiency Report Symbol Key (Table A3 below and in folder on the product CD) or directly from NIST 800-53 (in folder in folder on the product CD). In most cases the action plan will address upgrades in order of cost and convenience. Many changes are inexpensive and demonstrate progress to regulators without major cost. Other changes may require capital planning and be phased in over time.

For example, in the list above, SI-5 is Security Alerts and Advisories. A number of free websites can fill this need, including several government sites such as CERT. More information in this area is available from NIST Special Publications 800-40, 800-51, 800-61, as noted in the NIST 800-53 cross reference (in folder on the CD). On the other hand, CP-2, creating an NIST compliant Contingency Plan, can be a major effort. Guidance in this area can be found in NIST Special Publications 800-12, 800-14, 800-34, and 800-66 also included on your CD.

Deficiency Report

Risk Assessment Number 01-22-07-1169502566 - Report Generated January 22, 2007 - www.acr2solutions.com

Missing or Under-Performing Safeguards	E1	E2	E3	E4	E5	E6	HE1	HE2	HE3	HE4	HE5	HE6	HE7	HE8	MI1	MI2	MI3	MI4	MI5	MI6	MI7	MI8	MO1	MO2	MO3	MO4	MO5	MO6	MO7	MO8
AC-8							x	x	x	x	x		x	x																
AC-11							x	x	x	x	x		x	x	x	x	x	x	x		x	x	x	x	x	x	x		x	x
AC-13							x	x	x	x	x		x	x	x	x	x	x	x		x	x	x	x	x	x	x		x	x
AC-17							x	x	x	x	x		x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x
AC-18							x	x	x	x	x		x	x	x	x	x	x	x		x	x	x	x	x	x	x		x	x
AT-1							x	x	x	x	x		x	x																
AU-3							x	x	x	x	x		x	x	x	x	x	x	x		x	x	x	x	x	x	x		x	x
AU-9							x	x	x	x	x		x	x	x	x	x	x	x	x	x	x								
CA-1															x	x	x	x	x		x	x	x	x	x	x	x		x	x
CP-2	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
CP-8							x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
IA-1							x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
IA-4							x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
IR-3	x	x	x	x	x	x									x	x	x	x	x		x	x	x	x	x	x			x	x
MA-5																							x	x	x	x	x		x	x
MP-7							x	x	x	x	x				x	x	x	x	x				x	x	x	x	x			
PE-1	x	x	x	x	x	x						x																x		
PE-11	x	x	x	x	x	x																								
PL-3							x	x	x	x	x	x	x	x									x	x	x	x	x	x	x	x
PL-4							x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
PS-1															x	x	x	x	x	x	x	x								
PS-4															x	x	x	x	x	x	x	x								
PS-7															x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
RA-5							x	x	x	x	x				x	x	x	x	x	x	x	x	x	x	x	x	x		x	x
SA-6							x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
SA-9							x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
SC-4							x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
SC-7											x				x	x	x	x					x	x	x	x	x		x	x
SC-10											x								x								x			
SC-14											x								x								x			
SC-18											x								x				x	x	x	x	x			
SI-2							x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
SI-5							x	x	x	x	x				x	x	x	x	x				x	x	x	x	x		x	x
SI-11							x	x	x	x	x				x	x	x	x	x				x	x	x	x	x			
AutoPro							x	x	x	x	x			x	x	x	x	x	x		x	x	x	x	x	x	x	x		

Table A2: Deficiency Report

Summary

Once the action plan for the red risks is in place, then a similar program needs to be implemented for the yellow risks. Under NIST guidelines, risks in the yellow range need to be "scheduled for remediation". Again, the fastest and least expensive first rule of prioritization is a prudent use of limited corporate resources.

On a weekly basis, as new safeguards are implemented, the risk assessment can be updated with new reports. At a minimum, a monthly reassessment of risk is recommended, and should be placed in the appropriate portion of the organizations Information Security Plan notebook. Compliance regulators do not expect organizations to be perfectly secure, and perfect security is not required by regulations under GLBA, HIPAA or PCI. However, "reasonable and appropriate" progress is not only expected but required. Periodic, quantitative risk assessment reports can provide a low cost means of documenting the organization's compliance with the regulation

Automated Compliance Reporting Deficiency Report Symbol Key

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

Table A3: Deficiency Report Symbol Key