# ACR2 Basic Risk Assessment - Business Edition

# User Manual

ACR 2 Solutions, Inc.

# Table of Contents

# 1 Introduction

ACR2 Basic - Business Edition (Basic) is an automated system designed to simplify the process of creating and updating risk assessments. Risk assessment is the initial step required by most information security regulations, including the Gramm Leach Bliley Act (GLBA), the Federal Information Security Management Act (FISMA), the Payment Card Industry Data Security Standard (PCI DSS), and other state, federal and international information security standards.

Basic is designed around the protocols created by the United States National Institute of Standards and Technology (NIST). NIST procedures are rapidly becoming a de-facto standard. A partial set of the current NIST protocols for risk assessment is shown at right.

Automation of information security processes is essential for both adequate security and regulatory compliance. There are over 30,000 known vulnerabilities listed in the National Vulnerability Database (NVD), with more than 10 new vulnerabilities added daily. It is no longer practical to rely on general knowledge and manual checklists to secure an information system.

**Figure 1.1 A Partial Set of the NIST Protocols**

## 1.1 Typographical Conventions

This document uses the following typographical conventions:

- Command and option names appear in **bold** type in definitions and examples. The names of directories, files, machines, partitions, and volumes also appear in bold.
- User supplied information appears bolded inside **<angle brackets>.**
- Website addresses appear in Courier font.
- Hyperlinks appear underlined.
- Notational usage information appears in *italic* text.

# 2 Risk Management Overview

Risk assessment is a process that was largely developed in the environmental industry in the 1970s. As the federal government and other regulators realized the enormous benefits, they began requiring ever more organizations to conduct risk assessments- a practice which continues today. In 2002, the NIST produced a simplified risk assessment for use with "sensitive but unclassified" information stored by federal agencies and other regulated organizations.

NIST-compliant risk assessments are mandatory for organizations regulated under FISMA, and are recommended for those regulated by GLBA, the Health Insurance Portability and Accountability Act (HIPAA), and other information security regulations.

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

Other information security regulations have very similar requirements. Once a risk assessment has identified and quantified the risks to information security, it is possible to create an appropriate protection system.

Risk assessment involves review of vulnerabilities, probability of damage and the impact of damage. As discussed in the ACR white paper on risk assessment, it is possible to calculate risk scores using the NIST 800-30 protocol largely by comparing the network safeguards with the minimum standards established by NIST 800-53. Additional data includes UTM data, configuration scan data, and network policies.

Policy data and safeguards installations change at a slow rate. However, network configurations may change daily while UTM data changes on a minute to minute basis. It is now possible to automate the updating of risk assessment by automatically inputting data from the UTM and network scans on a daily basis. Policy changes may be added as they occur, creating the "near real-time" risk assessment that is the goal of NIST 800-39, the "flagship document of the NIST 800 series" (800-39, p. 42).

# 3 The ACR2™ Risk Reporting Process

ACR 2's second generation Automated Compliance Reporting (ACR2™) risk assessment combines information from an organization's existing Unified Threat Management (UTM) /Intrusion Prevention System (IPS), Anti-Virus (A/V) program, and a detailed NIST policy questionnaire to produce a quantitative, NIST compliant risk assessment. Risks are divided into environmental, human error, malicious insider and malicious outsider categories. Within each category, risks are rated from 1 (low) to 100, per the NIST 800-30 requirements.

The ACR2™ software operates on a remote server and is accessed through a secure web browser. The Software as a Service (SaaS) application allows for rapid updating as regulations, standards and the security environment change. Copies of the reference documents for the NIST protocols are contained on the CD that includes this User Manual.

ACR2™ users are not required to maintain a separate server system to support this component. Instead, inputs to the risk assessment are uploaded to ACR 2 Solutions' secure server for processing and maintaining risk assessment reports. At the end of the licensing period, the organization simply purchases additional licenses to continue utilizing the software.

> *Note: Inactive accounts will expire 1 year from the date of creation (typically the date the order was placed). Active accounts will expire 1 year from the date of activation.*

## 3.1 Collecting the Data

To complete a risk assessment, you will need access to and familiarity with

- The organization's Information Security Policy and Procedures
- Information about personnel with access to protected data
- Data from the organization's most recent UTM, IPS, and A/V scans

## 3.2 Accessing ACR2™ Basic

Browse to `https://www.acr2solutions.com/` and select the **Customer Login** tab.


**Figure 3.1 Customer Login**

You will be directed to the login screen. Enter the **Username** and **Password** (Serial Number) provided with the Basic CD, then click the **Login** button.

After the initial login, you will be required to change your **Password**. Because these passwords may be emailed, they are not secure and cannot be used for data entry. You must also enter the email address at which you wish to receive the risk assessment reports. If desired, username and/or verification information may also be changed.

*Note: Login information is case sensitive.*

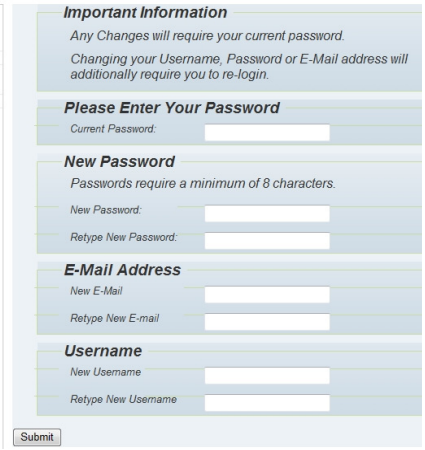


**Figure 3.2 Login Information screen**

After changing the account/verification information, you will be directed to login again, using the new information.

You will then be directed to the industry selection screen. This information will affect the typical regulatory scheme to be considered. While the overall risk assessment process is similar for a variety of regulations, there are differences in the details.

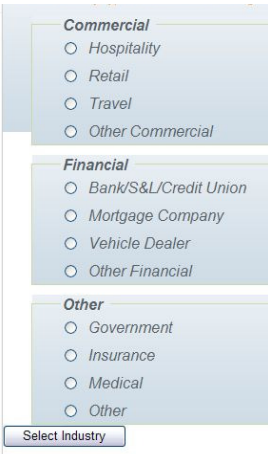


**Figure 3.3 Industry Selection screen**

After selecting an industry, you will be prompted to select additional regulations governing the organization's risk assessment. It is very common for organizations to be regulated under multiple sets of rules.

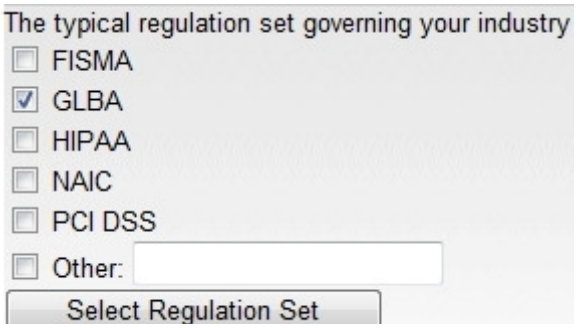


**Figure 3.4 Regulation Selection Screen**

After selecting the industry and regulatory environment, you can begin a Baseline Assessment. The Baseline is the first risk assessment of a calendar year, and all updated assessments will be compared to this assessment. Annual risk assessments are mandatory under most regulations.

Clicking **Start a New Baseline Assessment** brings up the **Disclaimer** page. Basic is a repackaging of NIST protocols, and is offered in good faith, but the disclaimer requires users to acknowledge that no warranty is offered or possible. ACR 2 Solutions, Inc. has no control over data entry, and therefore, cannot be held responsible for erroneous or misleading statements by our customers.

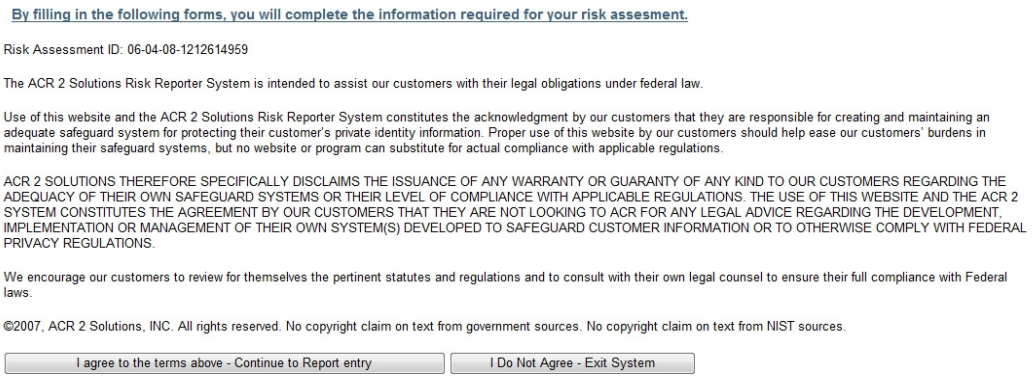


**Figure 3.5 Disclaimer screen**

*For enhanced security, risk assessment sessions will automatically timeout after 24 minutes on a single screen.*

## 3.3 Security Control Questions

The Questions section of the risk assessment pertains to the 170 Security Control questions contained in the NIST risk assessment (800-39) and minimum safeguards (800-53) protocols.

Each question is answered by selecting the most appropriate choice from the pull-down menu on the right. The options are **No** - the safeguard is not in place or functioning, **Yes** - the safeguard is in place and functioning, or **NA** - the safeguard does not apply at this location ( e.g. question AC-18: Wireless Access Restrictions for an organization that does not use wireless technology). The default answer for each question is No, the most conservative answer.

In general, the default answer for each question is No, the most conservative answer. However, following the upload of scan and UTM data, some questions may be answered Yes by default. These answers were populated based on the upload data. The user may also input data manually for these questions, overriding the upload data answer. For example, a compensating control may allow a Yes answer even if the scan data indicates otherwise.

*Note: If the organization is in substantial compliance, select Yes.*

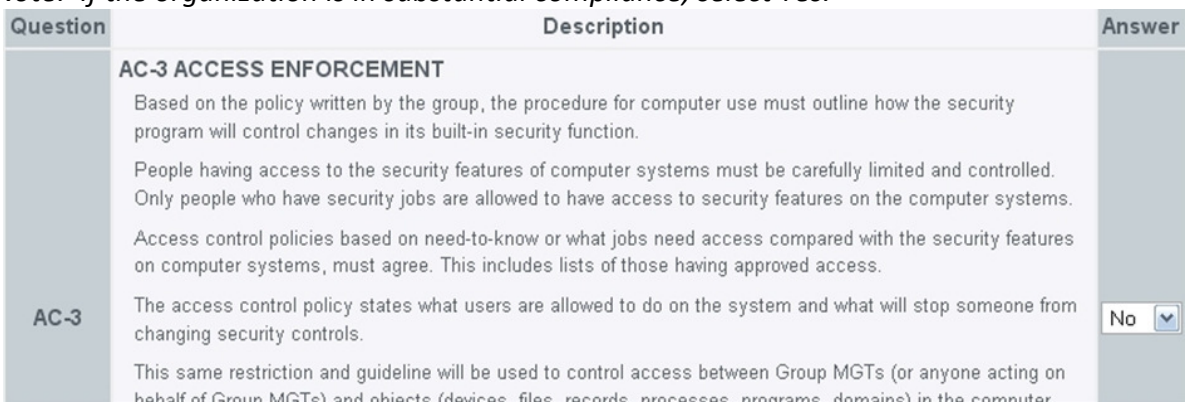


**Figure 3.6 Sample Question AC-3**

The language defining the safeguards is a plain English paraphrase of the original 18th grade NIST wording. To view the NIST wording for any safeguard, click the **Official Language** line at the end of the paraphrase. The official language for question AC-3 is shown below.


**Figure 3.7 Official Language Sample**

After answering the last question in a section, click the **Save and Continue** button. This is a secure transmission and may take up to a minute to load. Please do not click the button more than once.

This will bring up the next section requiring data input. The pull down menu at the top left of each data entry section can also be used to move from section to section of the program. While the order of data entry is completely under the user's control, it is necessary to finalize all of the sections to get the first report.

Depending upon your familiarity with the organization's Information Security Policy and Procedures, risk assessments may be completed in as few as three hours. However, risk assessments do not need to be completed in a single sitting. To interrupt a data session, use the **Log Out** line in the upper left corner of each data entry page. When you log back in, a new option to **Find and Complete Assessments** will appear on the login page.

*Note: Logging out will delete inputs to an unsubmitted data section. To save an incomplete data section, users must click the **Save and Continue** button.*

Selecting an incomplete risk assessment brings up a page that asks which group of questions you wish to address next. Click any group to bring up that data entry page. This selection is also a secure transaction which may take up to a minute to load.

## 3.4 UTM Data

This data entry section is different than the others; it requires numerical data and UTM/IPS, and A/V data.

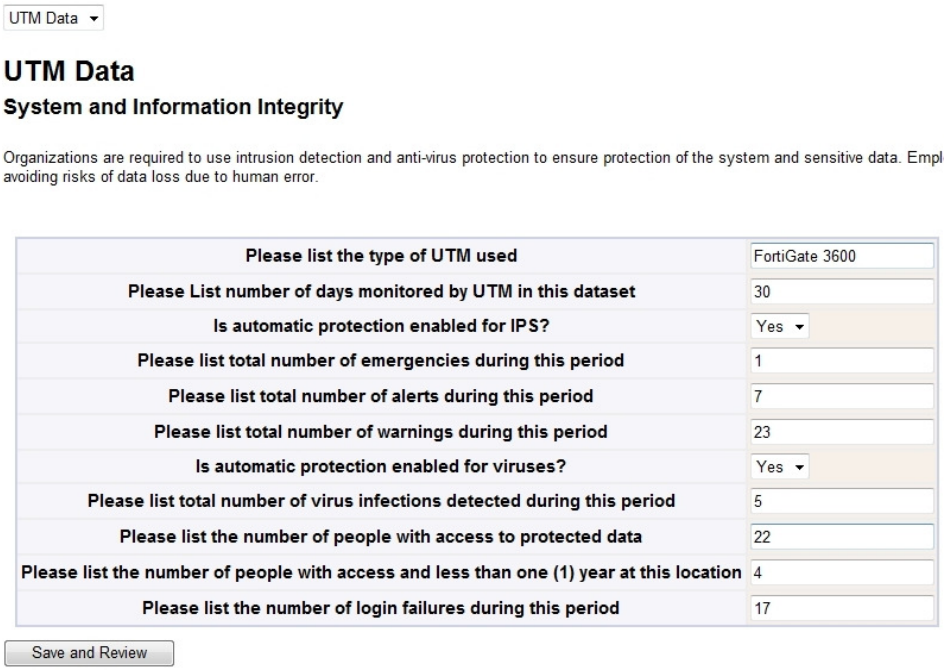


**Figure 3.8 UTM Data screen**

## 3.5 Data Review

The final section is the Review Screen. To review one section at a time, use the pull-down menu or click the blue section link. To view all questions at the same time, click the **Review All Answers** line above the Finalize button.

Once all of the sections have been updated, the **Finalize** button becomes active and a Baseline Report can be generated.

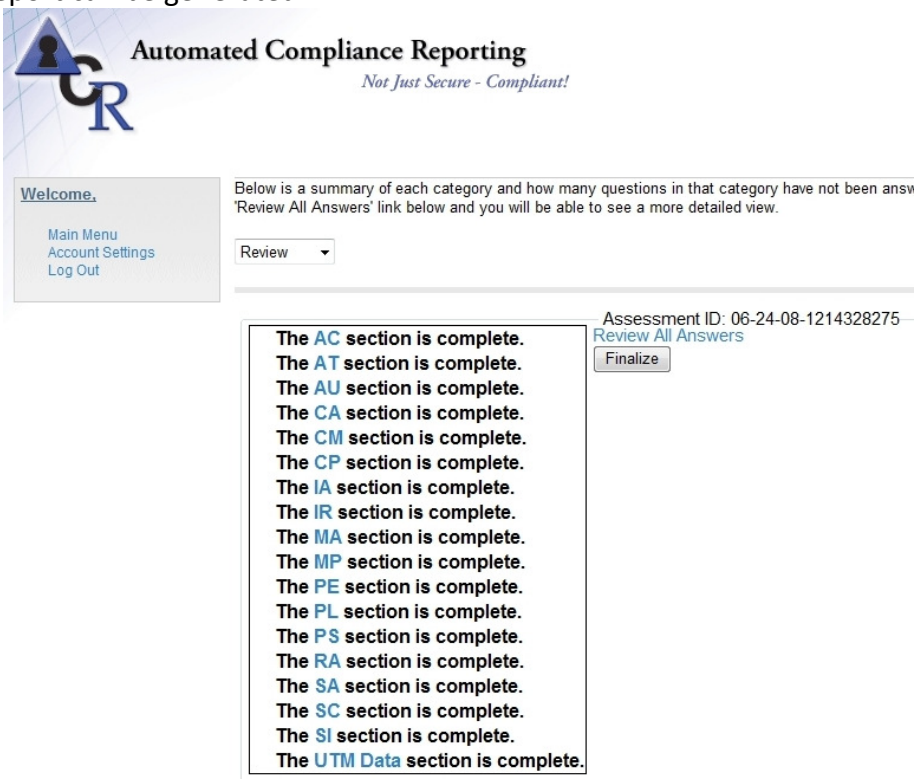


**Figure 3.9 Review screen**

## 3.6 The Results

ACR2™ reports are designed to help organizations efficiently prioritize and organize the safeguards that need updating and upgrading. 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. A risk score, from 1 (low) to 100 (high) is calculated by multiplying the likelihood score and the impact score.

According to NIST standards, risks scores > 50 need to be addressed immediately, risks scores 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 in the reports.

The risk assessment data will generate four encrypted reports, a Baseline Report, a Chart Report, a Status Report, and a Deficiency Report. These locked reports will be e-mailed to

the account that was specified during the account creation process, and require the ACR 2 account password to open.

A Gap Report, which is accessed from the Main Menu of the website, is also generated.

*Note: Access to e-mailed reports requires the installation of Adobe® Acrobat Reader® Version 6.0 or later.*

See Appendix A for report samples.

1. **baseline.pdf** - a numerical scoring of risks to information security and availability. Risks **are** defined as threat source/vulnerability combinations, and are divided into 30 risk categories based on the NIST protocols. Risks range from E1, wind/roof damage to MO8, malicious outsider/internal controls.

   The Baseline Report is the first report generated annually, and is used to determine the degree of change in future risk assessments. The Baseline report cannot be altered; additional risk assessments will instead generate an **update.pdf**.

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 this organization's safeguards compared to the minimum recommended standards for federally regulated networks under NIST.
4. **deficiency.pdf** - a cross listing of missing or underperforming safeguards with risk categories for this system at this time. This highly compact representation of needed improvements provides a single page snapshot of necessary changes.
5. **Gap Report** - a detailed listing of missing or underperforming safeguards which have negatively impacted this risk assessment. Holding the cursor over each safeguard gives more information about the threat source and affected vulnerability.

These reports enable user to more easily create an Action Plan for the organization.

# 4 Applying the Risk Assessment

Compliance is a continuously moving target; conducting a risk assessment is only part of the risk management process. Regulated firms are required to

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

Data from a network scan (800-30 section 3.1), IPS data, Antivirus data (Section 3.3), and policy data are input into the ACR2™ Risk Engine. This creates the Results Documentation (Section 3.9) and recommendations for change.

The changes in Controls are implemented and the changes added to the risk engine, along with updated Scan, IPS, and A-V data. This cycle can be easily done as often as daily, with reports on demand.

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

## 4.1 Creating an Action Plan

Following the review and acceptance of these risk reports by management, it is necessary to create an action plan. The plan should prioritize the needed safeguards in order to increase or maintain compliance with information security regulations.

Once the needed safeguards are identified, they can be listed using data from the Deficiency Report Symbol Key. The key can be found on p. 20 and on the 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, safeguard SI-5: Security Alerts and Advisories, is easy to update. A number of free websites can fill this need, including several government sites such as the US Computer Emergency Readiness Team (US-CERT). See NIST Special Publications 800-40, 800-51, and 800-61 for guidance.

On the other hand, CP-2: Creating a NIST Compliant Contingency Plan requires major effort. See NIST Special Publications 800-12, 800-14, 800-34, and 800-66 for guidance.

ACR2 software links deficiency items with businesses that can provide solutions to help organizations deal with the deficiency. For example, from the deficiency report, the user could click on AC-18 in the .pdf report to open the web page www.baisecurity.net/pdfs/bai-

mss-ids-ips.pdf. This page is for a service which directly addresses the wireless access restrictions addressed by AC-18. For more information, see NIST 800-53 on the CD.

Once the action plan for red risks is in place, a similar program needs to be implemented for 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 organization's Information Security Plan notebook.

Compliance regulators do not expect organizations to be perfectly secure. 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 level.

## 4.2 Creating an Update Report

Creating an update report is easy. Login to an account that has had a baseline report issued within the last 12 months and select **Find and Complete Assessments**.

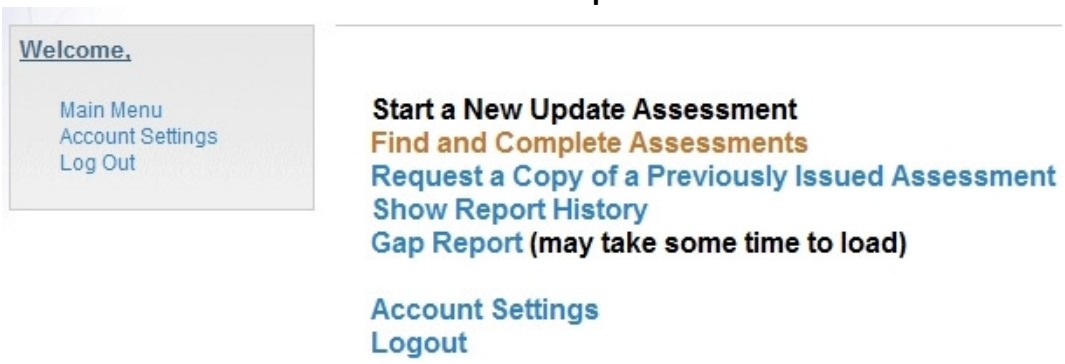


**Figure 4.1 Complete an Assessment**

As with the Baseline report, the data entry section begins after the disclaimer is accepted. The drop down menu can be used to change the assessment as needed. Once any known changes have been made, check the **Review** page to determine if any additional input is required.

From time to time changes are made in the NIST guidelines. When that occurs, sections that have been changed will show **Questions not reviewed** on the review page. These new questions must be answered before an update report is issued. The **Finalize** button brings up the report notice, completing the reporting cycle.

After multiple reports have been generated, options to **Request a Copy of a Previously Issued Assessment** and to **Show Report History** will become active.


**Figure 4.2 Additional Menu Options**

The **Show Report History** line will also be active. This screen allows you to analyze the changes that occur within subsequent risk assessments. Figure 4.3 shows an increased risk to E6. This report overview enables Compliance Officers to easily determine which Policies and Procedures changes affected the risk score. Click the blue **GO!** button to view each assessment and determine what changed.

## 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 leftm represent the scures of the indiviual reports. Click on the "GO" button near the top of the column to drill down to a specific here.

| ID | Assessment ID |
|---|---|
| A | 02-25-08-1203952881 |
| B | 03-29-08-1206802166 |
| C | 03-30-08-1206905063 |
| D | 03-30-08-1206905107 |
| E | 04-01-08-1207046846 |
| F | 04-01-08-1207057283 |
| G | 04-01-08-1207066423 |
| H | 06-24-08-1214328275 |

| ID | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| Type | Baseline | Update | Update | Update | Update | Update | Update | Update |
| Date | 03/20/08 | 04/02/08 | 06/24/08 | 06/24/08 | 06/24/08 | 06/24/08 | 06/24/08 | 06/26/08 |
| Risk | GO! | GO! | GO! | GO! | GO! | GO! | GO! | GO! |
| E1 | 25 | 25 | 25 | 25 | 25 | 25 | 25 | 25 |
| E2 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| E3 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 |
| E4 | 25 | 25 | 25 | 25 | 25 | 25 | 25 | 25 |
| E5 | 25 | 25 | 25 | 25 | 25 | 25 | 25 | 25 |
| E6 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 25 |
| HE1 | 25 | 25 | 25 | 25 | 25 | 25 | 25 | 25 |
| HE2 | 25 | 25 | 25 | 25 | 25 | 25 | 25 | 25 |
| HE3 | 25 | 25 | 25 | 25 | 25 | 25 | 25 | 25 |
| HE4 | 25 | 25 | 25 | 25 | 25 | 25 | 25 | 25 |
| HE5 | 25 | 25 | 25 | 25 | 25 | 25 | 25 | 25 |
| HE6 | 50 | 50 | 50 | 50 | 50 | 50 | 50 | 50 |
| HE7 | 25 | 25 | 25 | 25 | 25 | 25 | 25 | 25 |
| HE8 | 25 | 25 | 25 | 25 | 25 | 25 | 25 | 25 |
| MI1 | 25 | 25 | 25 | 25 | 25 | 25 | 25 | 25 |

**Figure 4.3 Report History**

# 5 Contact ACR 2 Solutions, Inc.

Thank you for your interest in ACR 2 Solutions. For general information, contact our main office:

ACR 2 Solutions, Inc.
3 East Main Street
Suite 1A
Buford, GA 30518-5778

info@acr2solutions.com or 1 866-667-6011.

## 5.1 License Renewal

Thank you for using ACR2™ products for your annual compliance report needs. We hope that you found this product helpful and invite you to choose ACR2™ products for all of your risk assessment needs.

Renewing your license for ACR2™ products is easy. Contact our sales department at sales@acr2solutions.com, or call (770) 904-0997.

## 5.2 Technical Support

Technical support for ACR2™ products is available 24 hours a day, 7 days a week. Please review the appropriate section of this manual before contacting technical support.

If the problem persists, e-mail support@acr2solutions.com or call toll-free 1-866-864-3450. When contacting support, please have the following information available:

- The version of ACR2™ software used
- The computer's browser and operating system

# Appendix A – Sample Reports

| | 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 |
| MI3 | Malicious insider | Data retrieval | M | M | 25 |
| MI4 | Malicious insider | Data modification | M | M | 25 |
| MI5 | Malicious insider | Data transmission | M | H | 25 |
| MI6 | Malicious insider | System design | M | M | 50 |
| MI7 | Malicious insider | Procedure implementation | M | M | 25 |
| MI8 | 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 |

**Baseline Report**

# Automated Update Report

Risk Assessment Number 05-14-08-1210791952 - Report Generated May 14, 2008 - www.riskreporterforfortinet.info

| | Date of Report | | 14-May-2008 | 14-May-2008 | |
|---|---|---|---|---|---|
| **Symbol** | **Threat Source** | **Vulnerability** | **Baseline Risk Score** | **Updated Risk Score** | **Change in Risk Score** |
| E1 | Wind | Roof damage | 100 | 1 | 99 |
| E2 | Fire | Smoke damage | 100 | 1 | 99 |
| E3 | Flood | Facility damage | 100 | 1 | 99 |
| E4 | Power loss | Loss of operations | 100 | 1 | 99 |
| E5 | Power loss | Damage to building | 100 | 1 | 99 |
| E6 | Vehicle collision | Facility damage | 100 | 1 | 99 |
| HE1 | Human error | Data acquisition | 100 | 25 | 75 |
| HE2 | Human error | Data storage | 100 | 25 | 75 |
| HE3 | Human error | Data retrieval | 100 | 25 | 75 |
| HE4 | Human error | Data modification | 100 | 25 | 75 |
| HE5 | Human error | Data transmission | 100 | 25 | 75 |
| HE6 | Human error | System design | 100 | 50 | 50 |
| HE7 | Human error | Procedure implementation | 100 | 25 | 75 |
| HE8 | Human error | Internal controls | 100 | 25 | 75 |
| MI1 | Malicious insider | Data acquisition | 100 | 25 | 75 |
| MI2 | Malicious insider | Data storage | 100 | 25 | 75 |
| MI3 | Malicious insider | Data retrieval | 100 | 25 | 75 |
| MI4 | Malicious insider | Data modification | 100 | 25 | 75 |
| MI5 | Malicious insider | Data transmission | 100 | 25 | 75 |
| MI6 | Malicious insider | System design | 100 | 50 | 50 |
| MI7 | Malicious insider | Procedure implementation | 100 | 25 | 75 |
| MI8 | Malicious insider | Internal controls | 100 | 25 | 75 |
| MO1 | Malicious outsider | Data acquisition | 50 | 5 | 45 |
| MO2 | Malicious outsider | Data storage | 50 | 5 | 45 |
| MO3 | Malicious outsider | Data retrieval | 50 | 5 | 45 |
| MO4 | Malicious outsider | Data modification | 50 | 5 | 45 |
| MO5 | Malicious outsider | Data transmission | 50 | 5 | 45 |
| MO6 | Malicious outsider | System design | 10 | 5 | 5 |
| MO7 | Malicious outsider | Procedure implementation | 100 | 50 | 50 |
| MO8 | Malicious outsider | Internal controls | 100 | 50 | 50 |

**Update Report**

# Risk Assessment Chart

Risk Assessment Number 05-14-08-1210791952 - Report Generated May 14, 2008 - www.riskreporterforfortinet.info

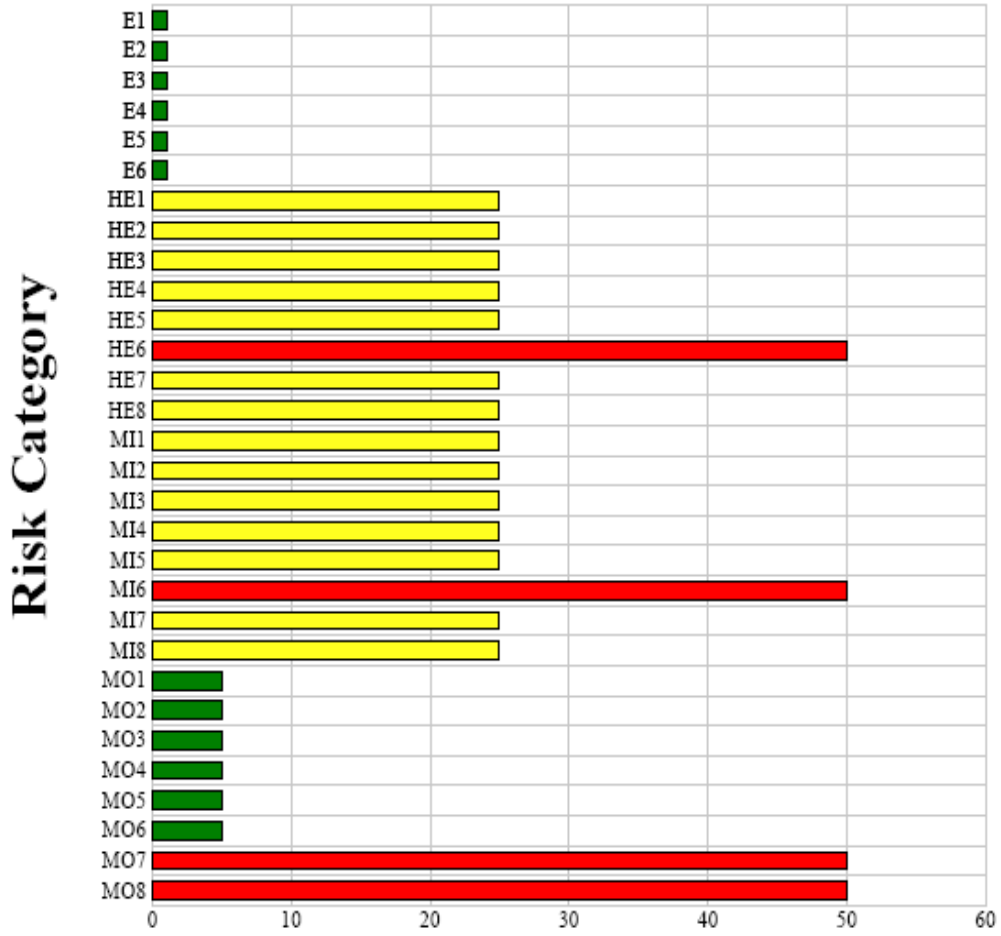


**Chart Report**

# Safeguard Status Report

Risk Assessment Number 05-14-08-1210791952 - Report Generated May 14, 2008 - www.riskreporterforfortinet.info

| SG | BaS | UpS | SG | BaS | UpS | SG | BaS | UpS | SG | BaS | UpS | SG | BaS | UpS | SG | BaS | UpS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AC-1 | No | Yes | AU-5 | No | Yes | CP-8 | No | No | PE-1 | No | Yes | PS-4 | No | No | SC-8 | No | No |
| AC-2 | No | No | AU-6 | No | Yes | CP-9 | No | Yes | PE-2 | No | Yes | PS-5 | No | No | SC-9 | No | No |
| AC-3 | No | No | AU-7 | No | No | CP-10 | Yes | Yes | PE-3 | No | Yes | PS-6 | No | Yes | SC-10 | No | No |
| AC-4 | No | No | AU-8 | No | No | IA-1 | No | No | PE-4 | No | No | PS-7 | No | Yes | SC-11 | No | No |
| AC-5 | No | Yes | AU-9 | No | No | IA-2 | No | No | PE-5 | No | No | PS-8 | Yes | Yes | SC-12 | No | Yes |
| AC-6 | No | No | AU-10 | No | Yes | IA-3 | No | Yes | PE-6 | No | Yes | RA-1 | No | Yes | SC-13 | No | Yes |
| AC-7 | No | No | AU-11 | Yes | Yes | IA-4 | No | Yes | PE-7 | No | Yes | RA-2 | No | Yes | SC-14 | No | No |
| AC-8 | No | No | CA-1 | No | Yes | IA-5 | No | No | PE-8 | No | Yes | RA-3 | No | Yes | SC-15 | No | Yes |
| AC-9 | No | Yes | CA-2 | No | Yes | IA-6 | No | No | PE-9 | No | No | RA-4 | No | Yes | SC-16 | No | Yes |
| AC-10 | No | No | CA-3 | No | Yes | IA-7 | Yes | Yes | PE-10 | No | No | RA-5 | Yes | Yes | SC-17 | No | No |
| AC-11 | No | No | CA-4 | No | Yes | IR-1 | No | Yes | PE-11 | No | Yes | SA-1 | No | Yes | SC-18 | No | No |
| AC-12 | No | Yes | CA-5 | No | Yes | IR-2 | No | Yes | PE-12 | No | Yes | SA-2 | No | Yes | SC-19 | No | Yes |
| AC-13 | No | Yes | CA-6 | No | Yes | IR-3 | No | Yes | PE-13 | No | Yes | SA-3 | No | Yes | SC-20 | No | No |
| AC-14 | No | NA | CA-7 | Yes | Yes | IR-4 | No | Yes | PE-14 | No | Yes | SA-4 | No | Yes | SC-21 | No | No |
| AC-15 | No | No | CM-1 | No | Yes | IR-5 | No | Yes | PE-15 | No | Yes | SA-5 | No | No | SC-22 | No | No |
| AC-16 | No | No | CM-2 | No | No | IR-6 | No | Yes | PE-16 | No | No | SA-6 | No | No | SC-23 | Yes | Yes |
| AC-17 | No | No | CM-3 | No | Yes | IR-7 | Yes | Yes | PE-17 | No | No | SA-7 | No | Yes | SI-1 | No | Yes |
| AC-18 | No | Yes | CM-4 | No | No | MA-1 | No | Yes | PE-18 | No | Yes | SA-8 | No | No | SI-2 | No | Yes |
| AC-19 | No | Yes | CM-5 | No | No | MA-2 | No | Yes | PE-19 | Yes | Yes | SA-9 | No | Yes | SI-3 | No | No |
| AC-20 | Yes | Yes | CM-6 | No | No | MA-3 | No | Yes | PL-1 | No | Yes | SA-10 | No | No | SI-4 | No | Yes |
| AT-1 | No | Yes | CM-7 | No | No | MA-4 | No | Yes | PL-2 | No | Yes | SA-11 | Yes | Yes | SI-5 | No | No |
| AT-2 | No | Yes | CM-8 | Yes | Yes | MA-5 | No | Yes | PL-3 | No | Yes | SC-1 | No | Yes | SI-6 | No | No |
| AT-3 | No | Yes | CP-1 | No | Yes | MA-6 | Yes | Yes | PL-4 | No | Yes | SC-2 | No | No | SI-7 | No | No |
| AT-4 | No | Yes | CP-2 | No | Yes | MP-1 | No | Yes | PL-5 | No | No | SC-3 | No | Yes | SI-8 | No | No |
| AT-5 | Yes | Yes | CP-3 | No | Yes | MP-2 | No | Yes | PL-6 | Yes | Yes | SC-4 | No | No | SI-9 | No | Yes |
| AU-1 | No | Yes | CP-4 | No | Yes | MP-3 | No | No | PS-1 | No | Yes | SC-5 | No | No | SI-10 | No | Yes |
| AU-2 | No | No | CP-5 | No | Yes | MP-4 | No | No | PS-2 | No | Yes | SC-6 | No | No | SI-11 | No | Yes |
| AU-3 | No | No | CP-6 | No | Yes | MP-5 | No | Yes | PS-3 | No | Yes | SC-7 | No | No | SI-12 | Yes | Yes |
| AU-4 | No | No | CP-7 | No | Yes | MP-6 | Yes | Yes | | | | | | | | | |

Key to **Labels**(bold type)

SG Safeguard label as defined by NIST 800-53 "Minimum Precautions"

**Status Report**

# Deficiency Report

Risk Assessment Number 05-14-08-1210791952 - Report Generated May 14, 2008 - www.riskreporterforfortinet.info

| 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-2 | | | | | | | x | x | x | x | x | | x | x | x | x | x | x | x | | x | x | x | x | x | x | x | | x | x |
| AC-3 | | | | | | | x | x | x | x | x | | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | | x | x |
| AC-4 | | | | | | | x | x | x | x | x | | x | x | x | x | x | x | x | | x | x | x | x | x | x | x | | x | x |
| AC-6 | | | | | | | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | | x | x |
| AC-7 | | | | | | | x | x | x | x | x | | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | | x | x |
| AC-8 | | | | | | | x | x | x | x | x | | x | x | | | | | | | | | | | | | | | | |
| AC-10 | | | | | | | x | x | x | x | x | | x | x | x | x | x | x | x | | x | x | 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-17 | | | | | | | x | x | x | x | x | | x | x | x | x | x | x | x | | x | x | x | x | x | x | x | x | x | x |
| AU-2 | | | | | | | x | x | x | x | x | | x | x | x | x | x | x | x | | x | x | 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-4 | | | | | | | x | x | x | x | x | | x | x | x | x | x | x | x | | x | x | x | x | x | x | x | | x | x |
| AU-7 | | | | | | | x | x | x | x | x | | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | | x | x |
| AU-8 | | | | | | | x | x | x | x | x | | x | x | | | | | | | | | | | | | | | | |
| AU-9 | | | | | | | x | x | x | x | x | | x | x | x | x | x | x | x | x | x | x | | | | | | | | |
| CM-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 |
| CM-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 |
| CM-5 | | | | | | | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| CM-6 | | | | | | | x | x | x | x | x | x | x | x | x | x | x | x | | | x | x | x | x | x | x | x | | x | x |
| CM-7 | | | | | | | 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-2 | | | | | | | x | x | x | x | x | x | x | x | x | x | x | x | | | x | x | x | x | x | x | x | | x | x |
| IA-5 | | | | | | | 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-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 |
| MP-3 | | | | | | | x | x | x | x | x | | | | x | x | x | x | x | | | | x | x | x | x | x | | | |
| MP-4 | | | | | | | x | x | x | x | x | | | | x | x | x | x | x | | | | x | x | x | x | x | | | |
| PE-5 | | | | | | | | | | | | | | | | | | | | | | | x | x | x | x | x | x | x | x |
| PE-9 | | | | | | | | | | | | | | | | | | | | | | | x | x | x | x | x | x | x | x |
| PE-10 | x | x | x | x | x | x | | | | | | | | | | | | | | | | | | | | | | | | |
| PE-16 | | | | | | | x | x | x | x | x | | | | x | x | x | x | x | | | | x | x | x | x | x | | | |
| PE-17 | | | | | | | x | x | x | x | x | | | | x | x | x | x | x | | | | x | x | x | x | x | | | |
| PS-4 | | | | | | | | | | | | | | | x | x | x | x | x | x | x | x | | | | | | | | |

**Deficiency Report**


Risk Reporter for Fortinet
Not Just Secure - Compliant!
Welcome,
Main Menu
Account Settings
Manual
White Papers:
Automating Risk Management
Log Out
Gap Report
Risk Assessment Number 05-14-08-1210791952 - Dynamically Generated June 24, 2008 - 67.192.150.146
Summary
Below is a list of safeguards which negatively impacted this risk assessment.
For more information on an individual risk, hold your cursor over the text for a tool tip
CM-2 BASELINE CONFIGURATION
High Risks Affected:
HE6, MI6, MO7, MO8
Medium Risks Affected:
Risk: MO8
Source: Malicious outsider
Vulnerability: Internal controls
HE1, HE2, HE3, HE4
MI3, MI4, MI5, MI7, MI8
Low Risks Affected:
MO1, MO2, MO3, MO4, MO5, MO6
Paraphrase:
The group writes and keeps up a basic system design or map of the computer system and an inventory of the system's parts.
The basic system design complies with the Federal Enterprise Architecture and the group's information system structural design.
The inventory of systems parts includes manufacturer, type, serial number, version number, and location.
Every time a new part is added to the computer, the basic system design map should be updated. This action can be automated using a program.
Official Wording:
CM-4 MONITORING CONFIGURATION CHANGES
High Risks Affected:

**Gap Report**

# Appendix B - Deficiency Report 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 |
| MI3 | Malicious Insider | Data Retrieval |
| MI4 | Malicious Insider | Data Modification |
| MI5 | Malicious Insider | Data Transmission |
| MI6 | Malicious Insider | System Design |
| MI7 | Malicious Insider | Procedure Implementation |
| MI8 | 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 |

# Appendix C – Glossary

| Term | Meaning |
|---|---|
| **Action Plan** | A plan to prioritize and upgrade system safeguards to maintain or increase compliance. |
| **Administrative Account** | An account with administrative permissions to one or more systems on a network. |
| **Administrative Scan Account** | Administrators may create these accounts specifically for the purpose of conducting ThreatGuard Scans. More complex networks may require the creation of several accounts. |
| **Baseline Report** | The first risk assessment of a calendar year. This contains a numerical scoring of risks to information security and availability. All future risk assessments will be compared to the Baseline report. |
| **Chart Report** | A graphical, color coded representation of the baseline or update risk scores. |
| **Compliance Officer** | The individual responsible for conducting the risk assessment. |
| **Deficiency Report** | A cross listing of missing or underperforming safeguards. |
| **Federal Enterprise Architecture (FEA)** | A business-based framework for government-wide improvement developed by the OMB. It is intended to ease efforts to move the federal government toward becoming citizen-centered, results-oriented, and market-based. |
| **Gap Report** | A chart indicating “gaps” in security compliance. This report specifies which questions/factors negatively impacted the Risk Assessment score. |
| **Group** | CEOs, Managers, etc. who are responsible for maintaining security compliance. |
| **Hub** | A device used to connect multiple networking cables together to make them act as one unit. |
| **Hyperlink (link)** | Clickable text or graphics that direct the user to another document (typically a website) or to another place within the same document. |
| **Internal Network** | The client’s network. |
| **Intrusion Detection System (IDS)** | Software or hardware that detects attacks on a computer or network, but is incapable of stopping data damage or retrieval. |

| | |
|---|---|
| **Intrusion Prevention System (IPS)** | Software or hardware that is capable of real-time prevention of an attack on a computer or network. |
| **Isolated Network** | Internal ACR 2 network. |
| **Magnus Navigator** | The client application that is used to configure and manage the Secutor Magnus server. |
| **Network Administrator** | The individual responsible for installing the system. This individual manages the local area communications network within an organization and, traditionally, is responsible for the configuration, maintenance, day-to-day operations, and installation of infrastructure components. |
| **Network Address Translation** | The process of passing network traffic through a router that re-writes the source and/or destination IP addresses. |
| **Risk** | The likelihood that a vulnerability will be exploited, modified by the impact of the exploitation. |
| **Risk Score Change** | Risk Scores may change due to changes in the safeguards an organization uses or because of safeguard performance. |
| **Software as a Service (SaaS)** | A sales model whereby access to the software application is hosted by the seller and the user is provided access via the Internet. |
| **Status Report** | A compilation of the current status of the safeguards for the information system. |
| **Substantial Compliance** | Several aspects of security compliance are covered in each question. If a majority of aspects are in place, the group is considered to be in substantial compliance and may answer “Yes” to the question. |
| **System Logging (Syslog)** | The transmittal of event messages and alerts across an IP network. Messages are sent by the operating system or application to report the current status of a process. |
| **Unified Threat Management (UTM)** | UTM is used to describe network firewalls that have many features in one box, including e-mail spam filtering, anti-virus capability, an intrusion detection (or prevention) system (IDS or IPS), and World Wide Web content filtering, along with the traditional activities of a firewall. |
| **Update Report** | Any report made after the Baseline report. Determines the degree of increase or decrease in compliance compared to the baseline. Update risk assessments are required after system changes. |
| **Vulnerability** | Areas where security is weak and is at risk of being exploited. |

20080620