ACR2Basic Quick Start Guide

This program provides all of the information needed to conduct an annual risk assessment in accordance with Federal protocols. Risk assessment is required by the Gramm Leach Bliley Act (GBLA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA) and the Payment Card Industry Data Security Standard (PCI DSS).

Overview - Risk assessment is a process that was largely developed in the environmental industry in the 1970s. In 2002, the National Institute of Standards and Technology produced a simplified version of risk assessment for use with “sensitive but unclassified” information stored by Federal agencies and other federally regulated organizations. The protocol is contained in NIST 800-30. NIST protocols are mandatory for organizations regulated under FISMA and are recommended under GLBA and HIPAA.

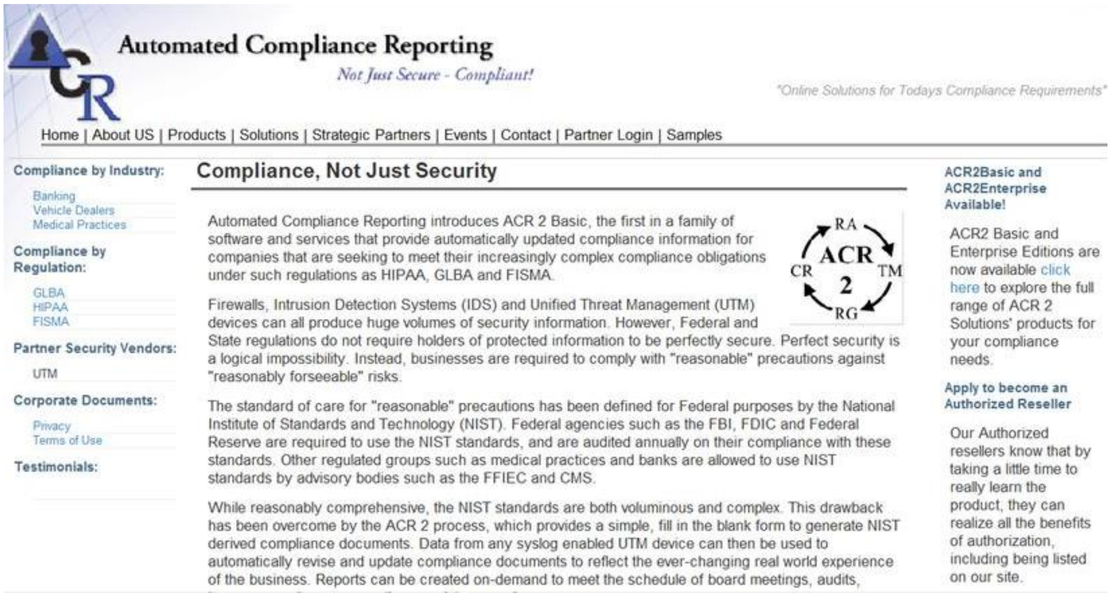
Summary Procedure - Protocol NIST 800-30 has a straightforward approach to assessing the overall risk environment of an information system.

Step 1. Identify basic system risks.
Step 2. Determine the likelihood of each risk and identify it as high, medium or low.
Step 3. Determine the impact of each risk, and identify it as high, medium or low.
Step 4 - Calculate a score for each risk. Risk scores range from 1 (low) to 100 (high).

Once the risks are characterized and scored, an action plan can be created.

Detailed Procedure - To create an ACR2Basic risk assessment it is necessary to connect to the Internet. It is recommended that users have a Windows™ PC using Windows 2000™ or later, a high speed Internet connection and a Windows Explorer™ 6 or later browser.

Go to the page www.acr2solutions.com.


Automated Compliance Reporting
Not Just Secure - Compliant!
"Online Solutions for Todays Compliance Requirements"
Home | About US | Products | Solutions | Strategic Partners | Events | Contact | Partner Login | Samples
Compliance by Industry:
Banking
Vehicle Dealers
Medical Practices
Compliance by Regulation:
GLBA
HIPAA
FISMA
Partner Security Vendors:
UTM
Corporate Documents:
Privacy
Terms of Use
Testimonials:
RA
ACR
2
CR
TM
RG

Compliance, Not Just Security

Automated Compliance Reporting introduces ACR 2 Basic, the first in a family of software and services that provide automatically updated compliance information for companies that are seeking to meet their increasingly complex compliance obligations under such regulations as HIPAA, GLBA and FISMA.

Firewalls, Intrusion Detection Systems (IDS) and Unified Threat Management (UTM) devices can all produce huge volumes of security information. However, Federal and State regulations do not require holders of protected information to be perfectly secure. Perfect security is a logical impossibility. Instead, businesses are required to comply with "reasonable" precautions against "reasonably forseeable" risks.

The standard of care for "reasonable" precautions has been defined for Federal purposes by the National Institute of Standards and Technology (NIST). Federal agencies such as the FBI, FDIC and Federal Reserve are required to use the NIST standards, and are audited annually on their compliance with these standards. Other regulated groups such as medical practices and banks are allowed to use NIST standards by advisory bodies such as the FFIEC and CMS.

While reasonably comprehensive, the NIST standards are both voluminous and complex. This drawback has been overcome by the ACR 2 process, which provides a simple, fill in the blank form to generate NIST derived compliance documents. Data from any syslog enabled UTM device can then be used to automatically revise and update compliance documents to reflect the ever-changing real world experience of the business. Reports can be created on-demand to meet the schedule of board meetings, audits,

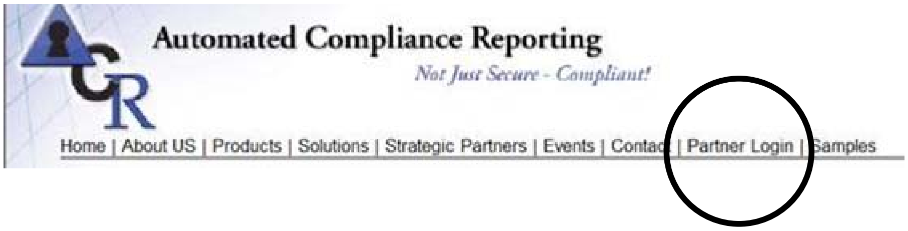
ACR2Basic and ACR2Enterprise Available!

ACR2 Basic and Enterprise Editions are now available click here to explore the full range of ACR 2 Solutions' products for your compliance needs.

Apply to become an Authorized Reseller

Our Authorized resellers know that by taking a little time to really learn the product, they can realize all the benefits of authorization, including being listed on our site.

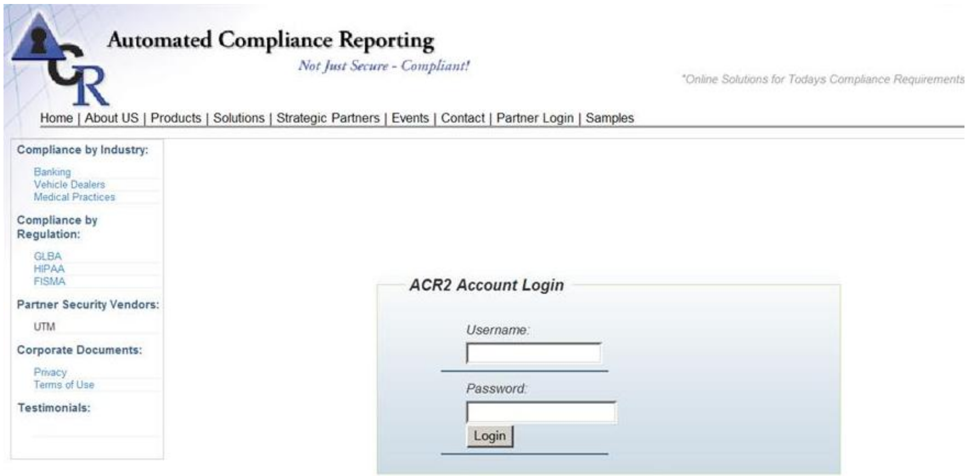
Click on the “Partner Login” tab on the home page


Automated Compliance Reporting
Not Just Secure - Compliant!
Home | About US | Products | Solutions | Strategic Partners | Events | Contact | Partner Login | Samples

This brings up the login screen

Type in your initial username and password. Note: both are case sensitive.

Then press the “Login” button.

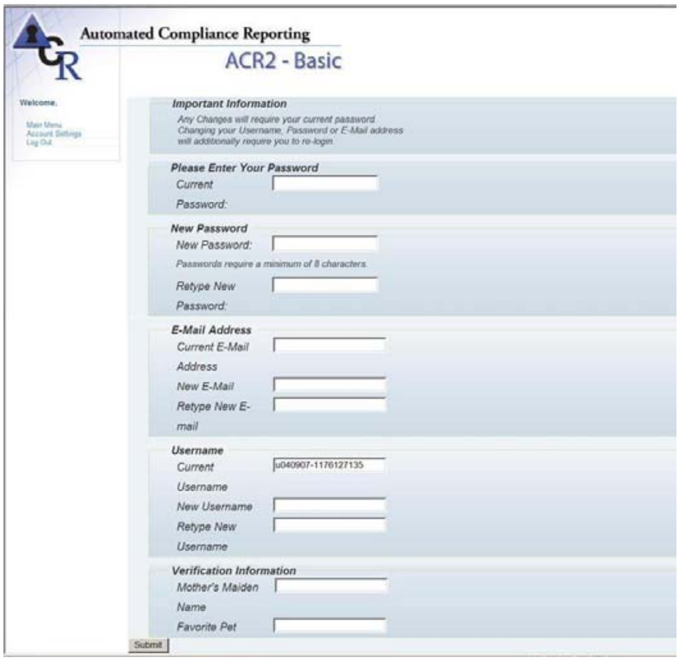

Automated Compliance Reporting
Not Just Secure - Compliant!
*Online Solutions for Todays Compliance Requirements
Home | About US | Products | Solutions | Strategic Partners | Events | Contact | Partner Login | Samples
Compliance by Industry:
Banking
Vehicle Dealers
Medical Practices
Compliance by Regulation:
GLBA
HIPAA
FISMA
Partner Security Vendors:
UTM
Corporate Documents:
Privacy
Terms of Use
Testimonials:

ACR2 Account Login

Username:

Password:

This will bring up the account settings page.



Important Information

Any Changes will require your current password
Changing your Username, Password or E-Mail address
will additionally require you to re-login

Please Enter Your Password

Current Password:

New Password

New Password:

Passwords require a minimum of 8 characters.

Retype New Password:

E-Mail Address

Current E-Mail Address

New E-Mail

Retype New E-mail

Username

Current Username: u040907-1176127135

New Username

Retype New Username

Verification Information

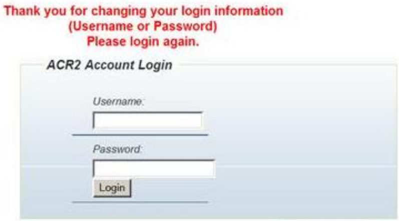
Mother's Maiden Name

Favorite Pet

The first time you enter the program, you must type in your current password and you must enter the email address at which you wish to receive your reports. Since initial passwords may in some cases be emailed, they are NOT SECURE and cannot be used for data entry. You MUST also change your password.

You may also change your username, and/or add verification information to your account.

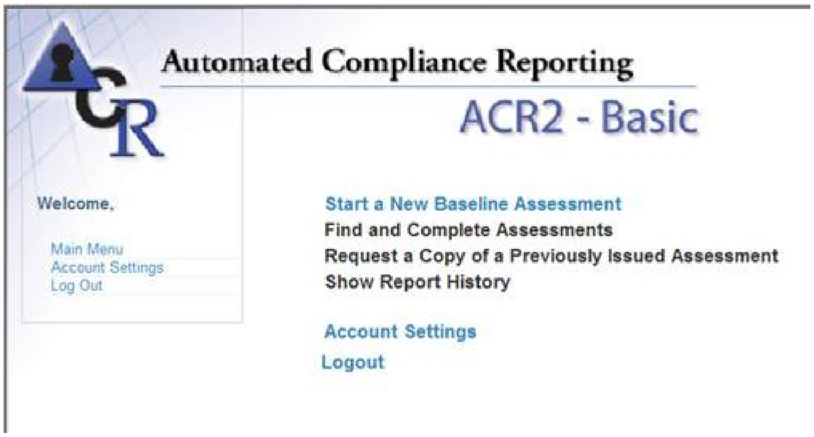
After changing your email, password, and username you will be directed to login with the new information.



Thank you for changing your login information
(Username or Password)
Please login again.

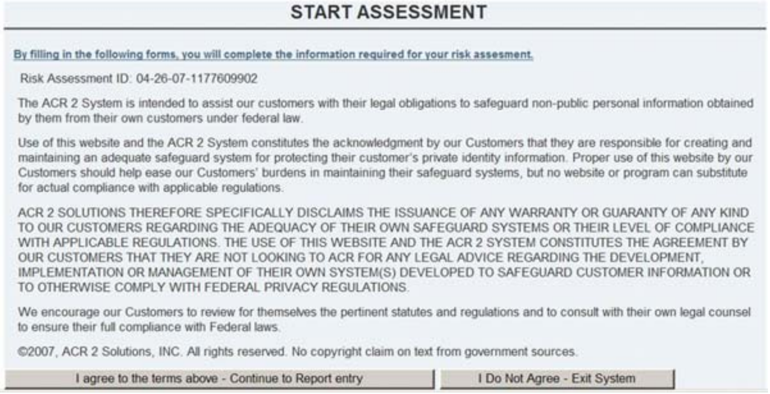
After logging in with your new password, you will proceed to the account home page. This is a home page exclusively for your account.

The first time you enter the account home page you can change your settings or begin a Baseline Assessment. The first risk assessment of a calendar year is the Baseline, and all updated assessments will be compared to this Baseline. Annual risk assessments are mandatory under several sets of Federal regulations.



Automated Compliance Reporting
ACR2 - Basic
Welcome,
Main Menu
Account Settings
Log Out
Start a New Baseline Assessment
Find and Complete Assessments
Request a Copy of a Previously Issued Assessment
Show Report History
Account Settings
Logout

Clicking on the “Start a New Baseline Assessment line brings up the Disclaimer page.



START ASSESSMENT

By filling in the following forms, you will complete the information required for your risk assesment.

Risk Assessment ID: 04-26-07-1177609902

The ACR 2 System is intended to assist our customers with their legal obligations to safeguard non-public personal information obtained by them from their own customers under federal law.

Use of this website and the ACR 2 System constitutes the acknowledgment by our Customers that they are responsible for creating and maintaining an adequate safeguard system for protecting their customer's private identity information. Proper use of this website by our Customers should help ease our Customers' burdens in maintaining their safeguard systems, but no website or program can substitute for actual compliance with applicable regulations.

ACR 2 SOLUTIONS THEREFORE SPECIFICALLY DISCLAIMS THE ISSUANCE OF ANY WARRANTY OR GUARANTY OF ANY KIND TO OUR CUSTOMERS REGARDING THE ADEQUACY OF THEIR OWN SAFEGUARD SYSTEMS OR THEIR LEVEL OF COMPLIANCE WITH APPLICABLE REGULATIONS. THE USE OF THIS WEBSITE AND THE ACR 2 SYSTEM CONSTITUTES THE AGREEMENT BY OUR CUSTOMERS THAT THEY ARE NOT LOOKING TO ACR FOR ANY LEGAL ADVICE REGARDING THE DEVELOPMENT, IMPLEMENTATION OR MANAGEMENT OF THEIR OWN SYSTEM(S) DEVELOPED TO SAFEGUARD CUSTOMER INFORMATION OR TO OTHERWISE COMPLY WITH FEDERAL PRIVACY REGULATIONS.

We encourage our Customers to review for themselves the pertinent statutes and regulations and to consult with their own legal counsel to ensure their full compliance with Federal laws.

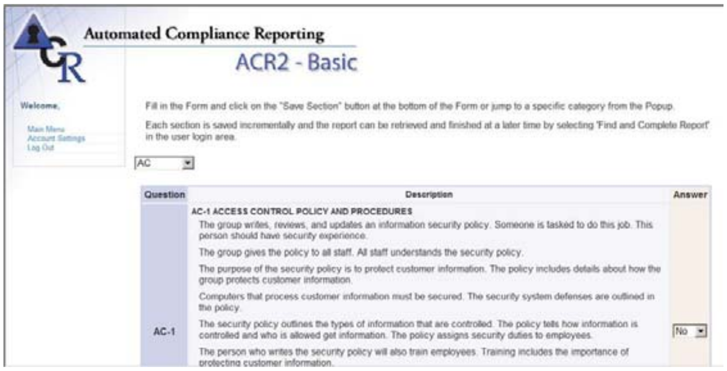
©2007, ACR 2 Solutions, INC. All rights reserved. No copyright claim on text from government sources.

I agree to the terms above - Continue to Report entry
I Do Not Agree - Exit System

ACR2 has no control over data entry by our customers and cannot be responsible for erroneous or misleading statements.

ACR2Basic is a repackaging of NIST protocols and is offered in good faith, but no warranty is offered or possible.

Pressing the “I agree” bar will bring up the first data entry screen. This screen asks the 20 access control questions contained in the NIST risk assessment and minimum safeguards protocols. There are about 92 protocols referenced in the NIST risk management protocols.



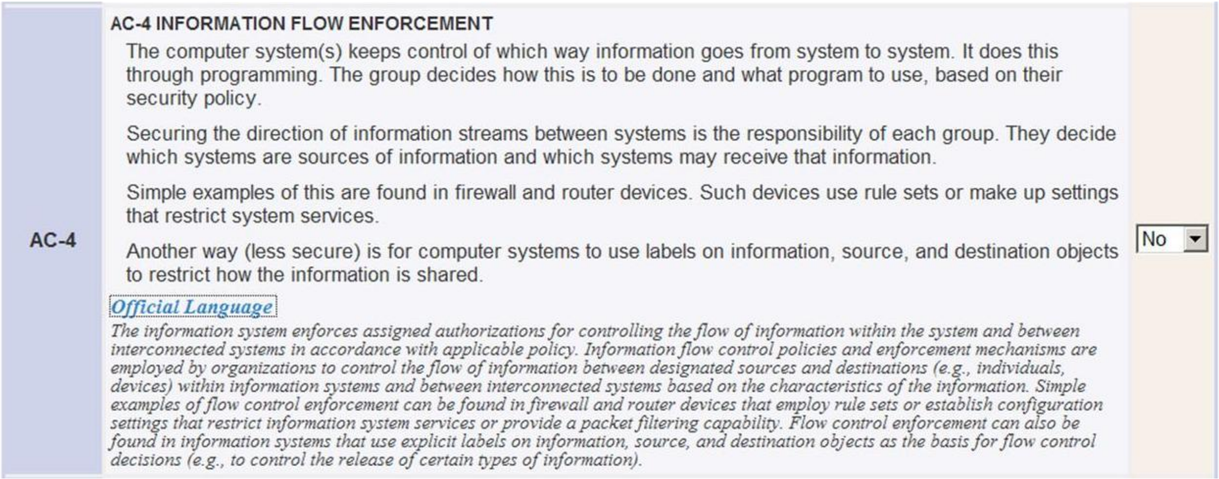
Fill in the Form and click on the "Save Section" button at the bottom of the Form or jump to a specific category from the Popup.

Each section is saved incrementally and the report can be retrieved and finished at a later time by selecting 'Find and Complete Report' in the user login area.

AC

Question	Description	Answer
AC-1	AC-1 ACCESS CONTROL POLICY AND PROCEDURES The group writes, reviews, and updates an information security policy. Someone is tasked to do this job. This person should have security experience. The group gives the policy to all staff. All staff understands the security policy. The purpose of the security policy is to protect customer information. The policy includes details about how the group protects customer information. Computers that process customer information must be secured. The security system defenses are outlined in the policy. The security policy outlines the types of information that are controlled. The policy tells how information is controlled and who is allowed get information. The policy assigns security duties to employees. The person who writes the security policy will also train employees. Training includes the importance of protecting customer information.	No

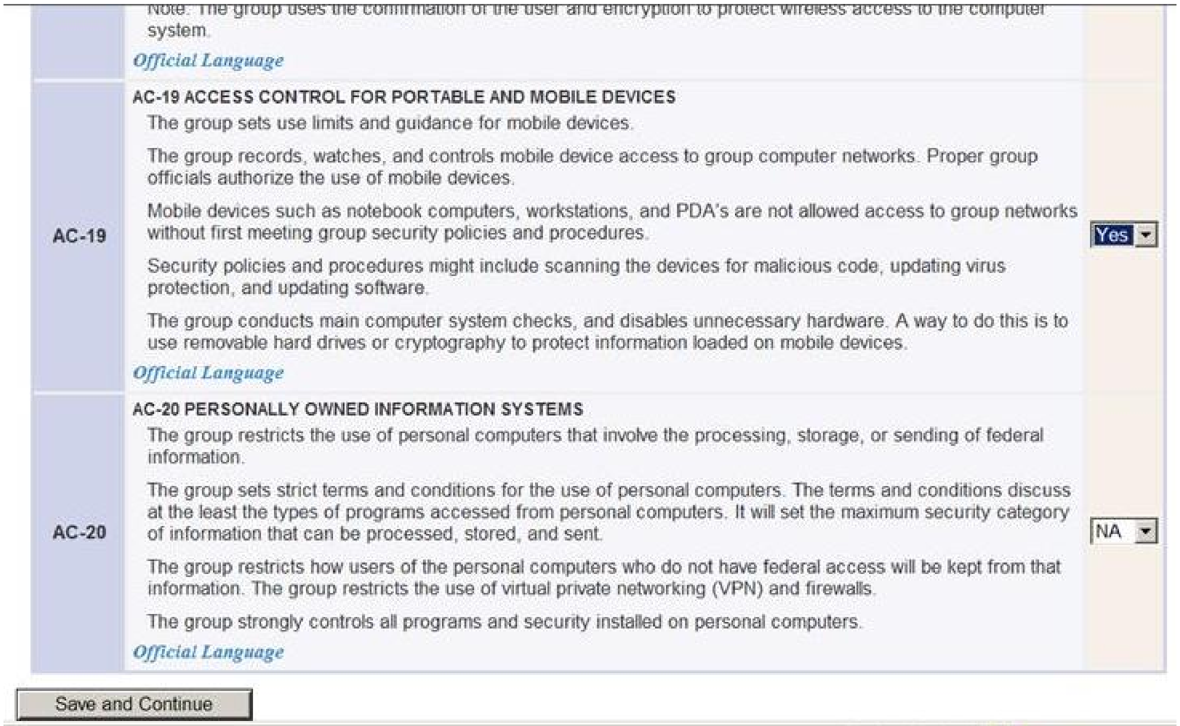
Choices from the pull-down menu are “No” the safeguard is not in place, “Yes” the safeguard is in place and functioning, or “NA” is does not apply at this location.



AC-4	**AC-4 INFORMATION FLOW ENFORCEMENT** The computer system(s) keeps control of which way information goes from system to system. It does this through programming. The group decides how this is to be done and what program to use, based on their security policy. Securing the direction of information streams between systems is the responsibility of each group. They decide which systems are sources of information and which systems may receive that information. Simple examples of this are found in firewall and router devices. Such devices use rule sets or make up settings that restrict system services. Another way (less secure) is for computer systems to use labels on information, source, and destination objects to restrict how the information is shared. *Official Language* *The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. Information flow control policies and enforcement mechanisms are employed by organizations to control the flow of information between designated sources and destinations (e.g., individuals, devices) within information systems and between interconnected systems based on the characteristics of the information. Simple examples of flow control enforcement can be found in firewall and router devices that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Flow control enforcement can also be found in information systems that use explicit labels on information, source, and destination objects as the basis for flow control decisions (e.g., to control the release of certain types of information).*	No ▾

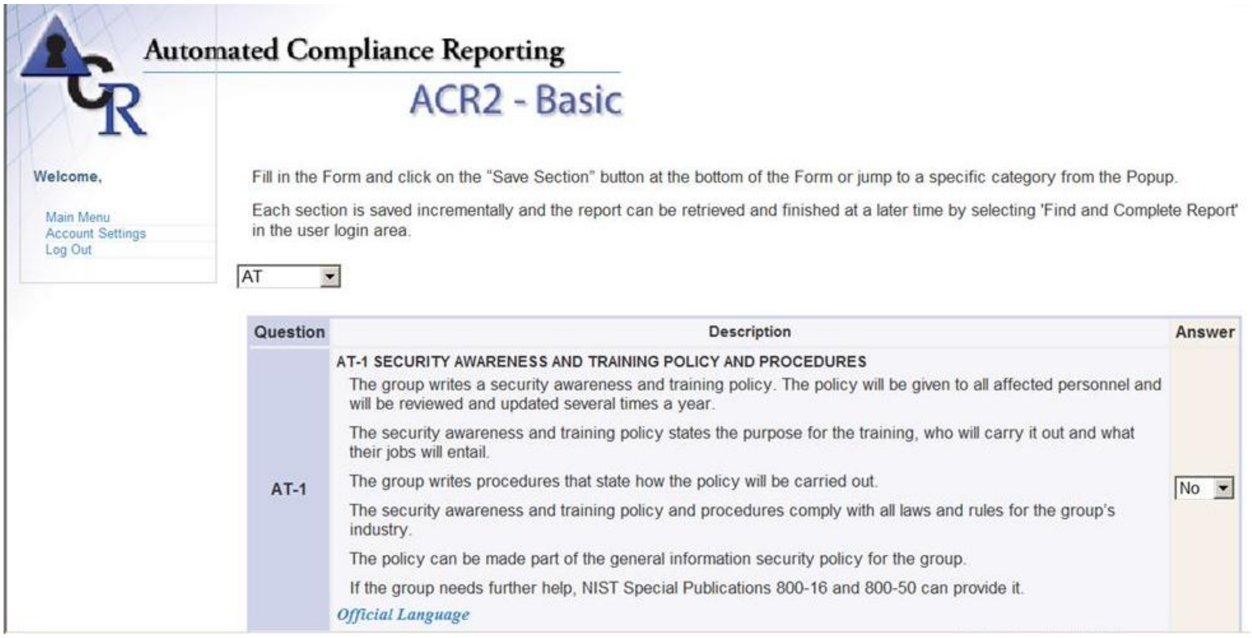
The language defining the safeguards is a 10th grade English paraphrase of the 18th grade NIST original language. The original NIST language is available for each safeguard by pressing the "official language" line at the end of each paraphrase. This is shown above for AC-4

After answering the last question in the AC section, you may press the "Save and Continue" button at the end of the section. This will move you to the next section of the data input.



	Note: The group uses the confirmation of the user and encryption to protect wireless access to the computer system. *Official Language*	
AC-19	**AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES** The group sets use limits and guidance for mobile devices. The group records, watches, and controls mobile device access to group computer networks. Proper group officials authorize the use of mobile devices. Mobile devices such as notebook computers, workstations, and PDA's are not allowed access to group networks without first meeting group security policies and procedures. Security policies and procedures might include scanning the devices for malicious code, updating virus protection, and updating software. The group conducts main computer system checks, and disables unnecessary hardware. A way to do this is to use removable hard drives or cryptography to protect information loaded on mobile devices. *Official Language*	Yes ▾
AC-20	**AC-20 PERSONALLY OWNED INFORMATION SYSTEMS** The group restricts the use of personal computers that involve the processing, storage, or sending of federal information. The group sets strict terms and conditions for the use of personal computers. The terms and conditions discuss at the least the types of programs accessed from personal computers. It will set the maximum security category of information that can be processed, stored, and sent. The group restricts how users of the personal computers who do not have federal access will be kept from that information. The group restricts the use of virtual private networking (VPN) and firewalls. The group strongly controls all programs and security installed on personal computers. *Official Language*	NA ▾

This is a secure transmission and may take up to a minute. Please do not press "Save and Continue" more than once.

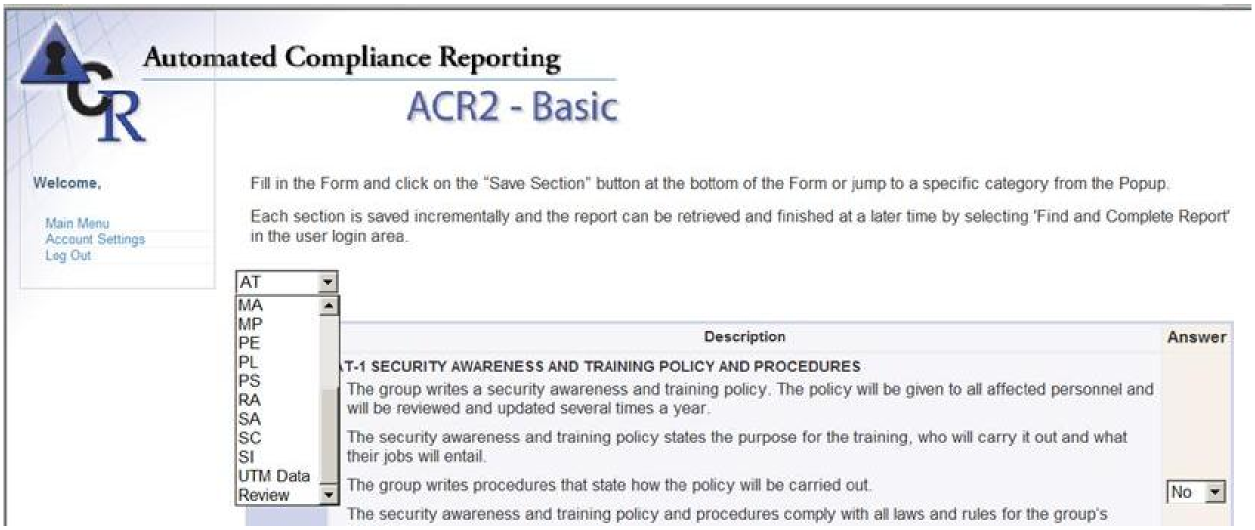


Fill in the Form and click on the "Save Section" button at the bottom of the Form or jump to a specific category from the Popup.

Each section is saved incrementally and the report can be retrieved and finished at a later time by selecting 'Find and Complete Report' in the user login area.

Question	Description	Answer
AT-1	**AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES** The group writes a security awareness and training policy. The policy will be given to all affected personnel and will be reviewed and updated several times a year. The security awareness and training policy states the purpose for the training, who will carry it out and what their jobs will entail. The group writes procedures that state how the policy will be carried out. The security awareness and training policy and procedures comply with all laws and rules for the group's industry. The policy can be made part of the general information security policy for the group. If the group needs further help, NIST Special Publications 800-16 and 800-50 can provide it. *Official Language*	No

Completing a baseline risk assessment requires completion of all sections addressed by the NIST. However, they do not have to be done in one sitting or in sequential order. Any of the sections may be addressed by using the drop down menu at the start of each data entry section.



Fill in the Form and click on the "Save Section" button at the bottom of the Form or jump to a specific category from the Popup.

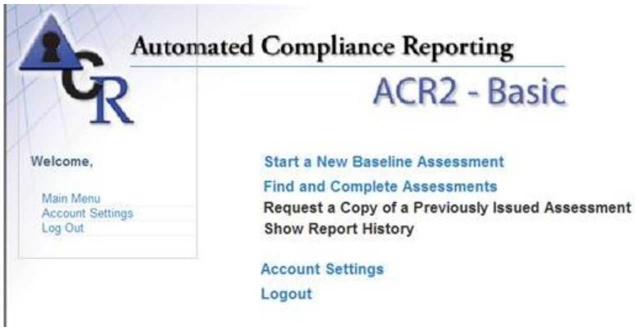
Each section is saved incrementally and the report can be retrieved and finished at a later time by selecting 'Find and Complete Report' in the user login area.

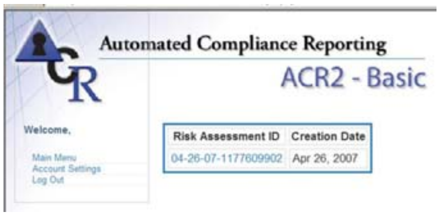
Description	Answer
T-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES The group writes a security awareness and training policy. The policy will be given to all affected personnel and will be reviewed and updated several times a year. The security awareness and training policy states the purpose for the training, who will carry it out and what their jobs will entail. The group writes procedures that state how the policy will be carried out. The security awareness and training policy and procedures comply with all laws and rules for the group's	No

A full risk assessment takes about three hours in one of our seminars. Updating the risk assessment usually takes only a few minutes, and is often done monthly to prepare for Board meetings, particularly in banks.

To interrupt a data session, use the "Log Out" line in the upper right corner of each data entry page. When you log back in, whether an hour or a week later, a new option will appear on the login page.

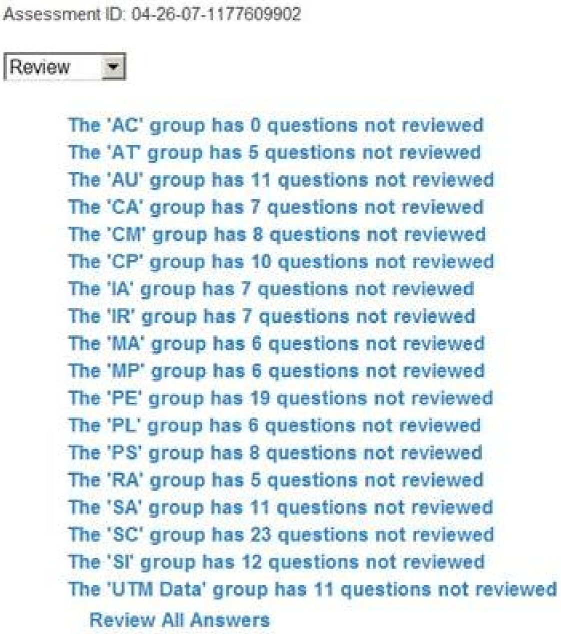
At this point, you may complete your earlier risk assessment or begin a new baseline from scratch.


Automated Compliance Reporting
ACR2 - Basic
Welcome,
Main Menu
Account Settings
Log Out
Start a New Baseline Assessment
Find and Complete Assessments
Request a Copy of a Previously Issued Assessment
Show Report History
Account Settings
Logout



Risk Assessment ID	Creation Date
04-26-07-1177609902	Apr 26, 2007

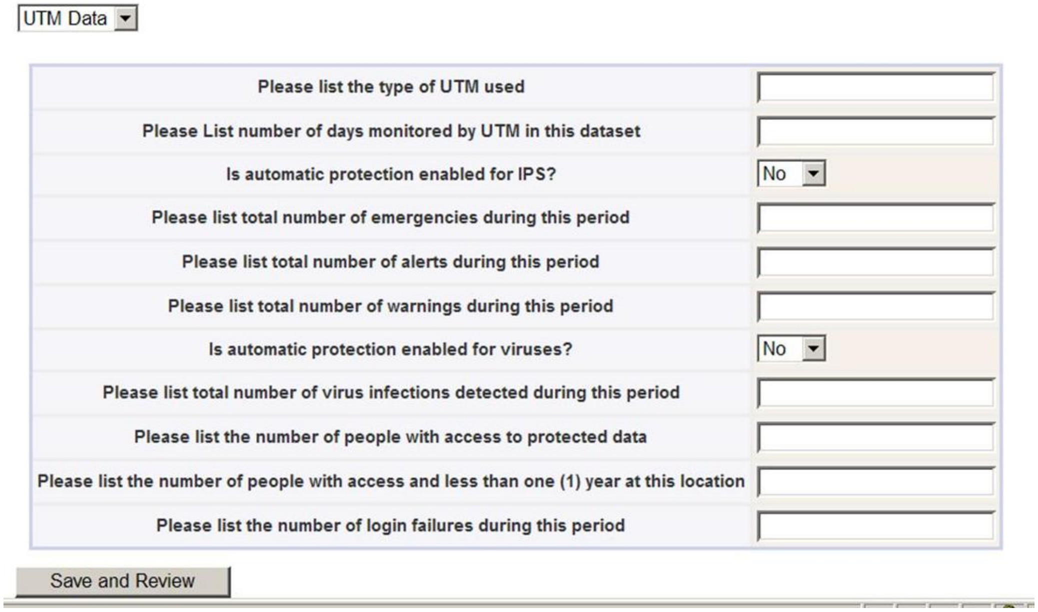
Selecting an uncompleted risk assessment brings up the screen to right, where the program asks which group of questions you wish to address next. Clicking on a group brings up the data entry page. The selection is a secure transaction which may take up to a minute.


Assessment ID: 04-26-07-1177609902

The 'AC' group has 0 questions not reviewed
The 'AT' group has 5 questions not reviewed
The 'AU' group has 11 questions not reviewed
The 'CA' group has 7 questions not reviewed
The 'CM' group has 8 questions not reviewed
The 'CP' group has 10 questions not reviewed
The 'IA' group has 7 questions not reviewed
The 'IR' group has 7 questions not reviewed
The 'MA' group has 6 questions not reviewed
The 'MP' group has 6 questions not reviewed
The 'PE' group has 19 questions not reviewed
The 'PL' group has 6 questions not reviewed
The 'PS' group has 8 questions not reviewed
The 'RA' group has 5 questions not reviewed
The 'SA' group has 11 questions not reviewed
The 'SC' group has 23 questions not reviewed
The 'SI' group has 12 questions not reviewed
The 'UTM Data' group has 11 questions not reviewed
Review All Answers

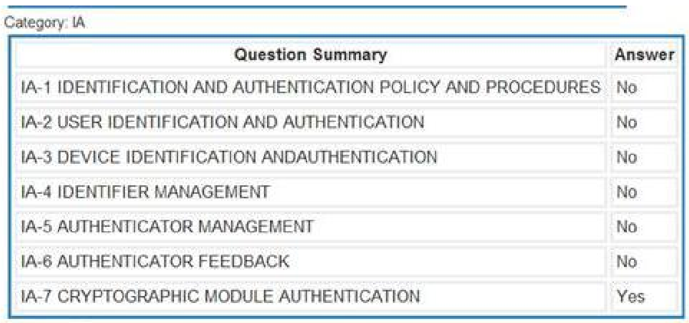
For each annual baseline report, all 18 of the sections of data input must be addressed. The default answer for each dropdown question is “no”, which is the most conservative option.

The last data entry section is slightly different from the others in that it includes numerical data on the intrusion detection and anti-virus performance of the system, if any. It is assumed that typically a Unified Threat Management (UTM) device such as the Fortigate FG-60 is used, but data from a combination of packet inspection firewall and desktop anti-virus could also be used. If no such protection is present, list the type of UTM as “none”.



Please list the type of UTM used	
Please List number of days monitored by UTM in this dataset	
Is automatic protection enabled for IPS?	No
Please list total number of emergencies during this period	
Please list total number of alerts during this period	
Please list total number of warnings during this period	
Is automatic protection enabled for viruses?	No
Please list total number of virus infections detected during this period	
Please list the number of people with access to protected data	
Please list the number of people with access and less than one (1) year at this location	
Please list the number of login failures during this period	

Once all the data has been put into the system a report may be requested. All data input may be reviewed at any time prior to submittal.

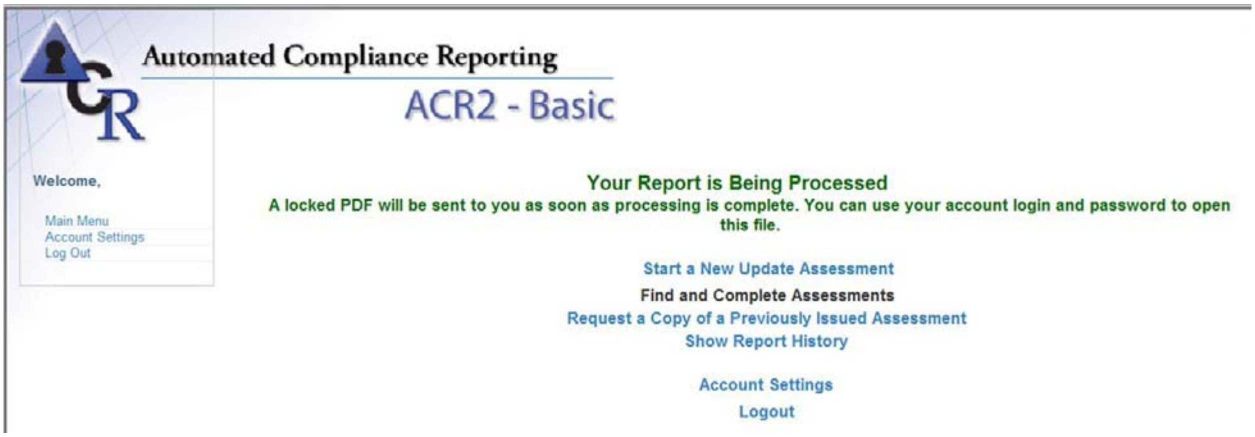


Category: IA

Question Summary	Answer
IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	No
IA-2 USER IDENTIFICATION AND AUTHENTICATION	No
IA-3 DEVICE IDENTIFICATION ANDAUTHENTICATION	No
IA-4 IDENTIFIER MANAGEMENT	No
IA-5 AUTHENTICATOR MANAGEMENT	No
IA-6 AUTHENTICATOR FEEDBACK	No
IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION	Yes

Once a report is requested, a PDF document set similar to that on the “Samples” page of the ACR 2 Solutions website is generated and emailed to the user of the software. All PDF reports are encrypted using the data entry login password.

Following data review, the “Finalize” button becomes active and an initial baseline report is generated.



Automated Compliance Reporting

ACR2 - Basic

Welcome,

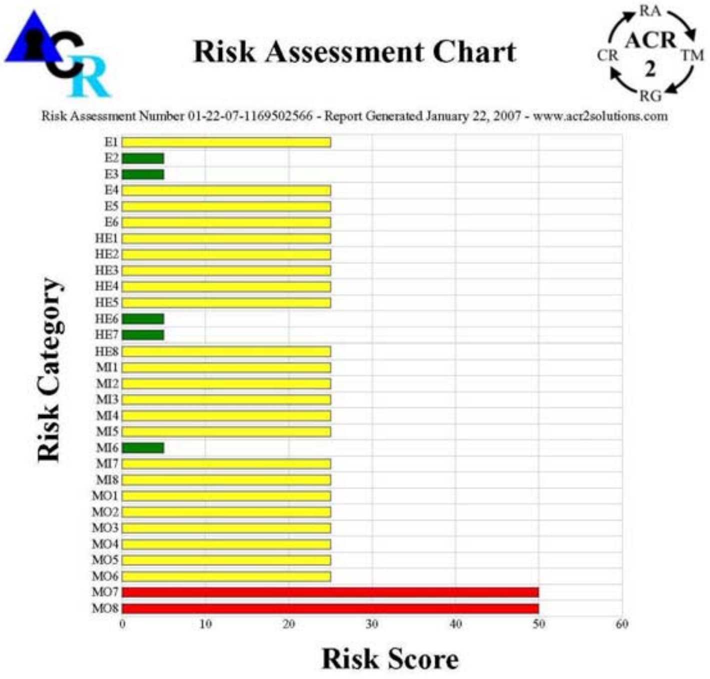
Your Report is Being Processed

A locked PDF will be sent to you as soon as processing is complete. You can use your account login and password to open this file.

Main Menu
Account Settings
Log Out
Start a New Update Assessment
Find and Complete Assessments
Request a Copy of a Previously Issued Assessment
Show Report History
Account Settings
Logout

Once an initial baseline report is created, an update to that report may be created at any time in a calendar year from the initial report. Only one baseline is allowed per account, but updates may be created weekly.

Risk assessment is a difficult and poorly understood task for many organizations. By using the ACR2Basic software to automate the NIST protocols, any organization can have a simple and robust risk assessment process that meets or exceeds Federal standards.



Risk Assessment Chart

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

Please email any questions or comments to info@acr2solutions.com.