Cybersecurity for Small Manufacturing Organizations - Quickstart Guide

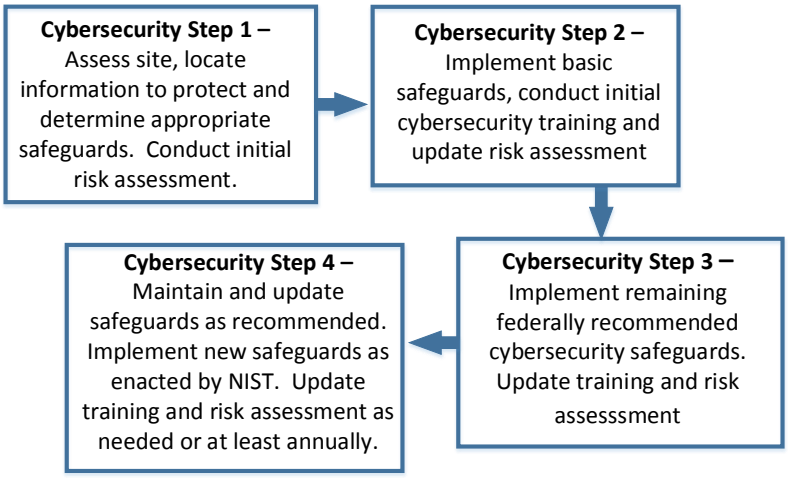
Overview

This software and services package was developed by cybersecurity consultants from ACR 2 Solutions (ACR 2) and our ACR Partners to assist small manufacturing organizations meet federal cybersecurity requirements for protecting sensitive medical, financial or operational information. A small manufacturer is defined as a single location employer with 200 or fewer employees.

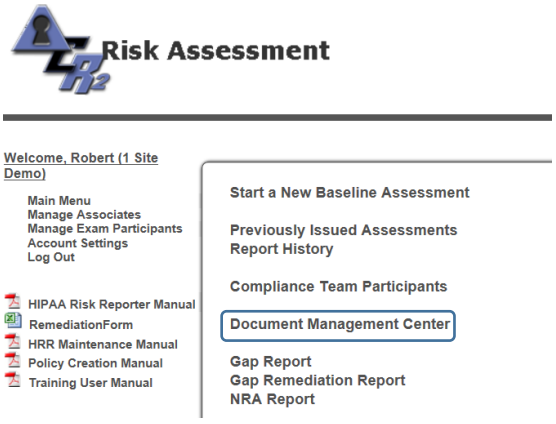
Many of the resources needed for achieving the task are provided in the cybersecurity risk management portal provided by ACR 2 Solutions. Using an internet browser such as Mozilla Firefox or Google Chrome, access the secure portal at www.multiple.riskassess.complianceobjects.com Enter the supplied username and password obtained from ACR 2. If you do not have these credentials, contact sales@acr2solutions.com .

There are **four steps** to bringing a small manufacturing organization into acceptable levels of cybersecurity as defined by federal standards of the National Institute of Standards and Technology or NIST.

Step 1 – Initial Cybersecurity Assessment and Comparison to Federal Standards.
Step 2- Implement Basic Cybersecurity Safeguards
Step 3 – Implement Full Federally Recommended Cybersecurity Program
Step 4 – Continue and Maintain Federally Recommended Cybersecurity Safeguards



Each step is detailed individually below.



Step 1 – Initial Cybersecurity Assessment and Federal Recommendations

a. Complete a Non-Disclosure Agreement (NDA). IF you haven't completed the NDA, a blank NDA form is located in the ACR 2 document repository. Login to the secure webportal previously noted with the username and password within the license from ACR 2. Click on "Document Management Center" (shown at left) to obtain your NDA form.

b. Identify and inventory data to be protected. Determine FIPS 199 classification – Low, Moderate or High. CUI is rated Moderate by definition, while typically medical or financial data is rated FIPS 199 High).

c. Locate data to be protected. Typically on servers, work stations, in cloud and/or file cabinets.
d. Obtain diagram of computer network with protected data locations.

These activity can be subcontracted to ACR 2 Partners. The ACR 2 Partners service will also include an inventory of devices on the network with IP addresses, including devices such as printers, workstations and servers.

e. Count current and potential users. Users are persons with current or potential access to protected information. Typically includes anyone using a computer with access to this data.
f. List current cybersecurity precautions – typically includes username/password access control, desktop antivirus, data backup, perimeter defenses i.e. firewall and physical safeguards.
g. Document existing cybersecurity precautions using the ACR 2 Policy Forms found in the risk assessment document repository. Forms are available for CUI, HIPAA and Cybersecurity Framework sites.

NIST 800-66, "An Introductory Resource Guide to Implementing the HIPAA Security Guide", NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" and the NIST "Framework for Improving Critical Infrastructure Cybersecurity" all map specific sets of cybersecurity requirements to some subset of the 906 standardized safety controls in NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations".

For example in NIST 800-171 Appendix D, as shown below, CUI requirement 3.8.9 is listed as mapping to NIST Special Publication 800-53 safeguard CP-9 on data backup.

CUI SECURITY REQUIREMENTS		NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	MP-7(1)	Media Use *Prohibit Use Without Owner*	*No direct mapping.*	
3.8.9	Protect the confidentiality of backup CUI at storage locations.	CP-9	Information System Backup	A.12.3.1	Information backup
				A.17.1.2	Implementing information security continuity
				A.18.1.3	Protection of records

The color coded ACR 2 Cybersecurity Policy Forms organize and summarize guidance from the any of these NIST documents. ACR 2 Policy Forms are available for recommended NIST security controls for HIPAA, CUI and Cybersecurity Framework sites, all of which use overlapping lists of NIST 800-53 safeguards.

Using the ACR 2 Policy Forms is simple. Read and erase explanatory text in blue. Fill in the data in red and recolor it black. Review the suggested policy clauses in black and modify as desired to meet local conditions. Have the compliance officer or other designated authority sign, date and disseminate the new local policy. Scan and upload the executed document to the Document Management Center. The newly adopted form will then be available to users during the online, on-demand Cybersecurity Awareness Training that is required of all users during Step 2 of the Cybersecurity Compliance process.

ACR 2 Cybersecurity Policy Forms are typically 2 or three pages long, although some are only 1 page and a few may be as long as 7 pages. As an example CUI Cybersecurity Policy Form 3.1.11 is shown in its' entirety on the following page

NIST 800-171 CUI Cybersecurity Policy/Procedure Form 3.1.11

3.1.11 Terminate (automatically) a user session after a defined condition.

General Instructions:

1. Replace all items in red with the information appropriate for your organization, deleting brackets and unused options as needed.
2. Delete these instructions and all others in blue when you have finished with them.
3. Modify text in black, if appropriate, to add, modify or delete wording according to the needs of your organization.
4. Review document and ensure that all remaining text is in black.
5. Document and Disseminate - Once the policy has been approved, print, sign/date as indicated at the bottom of the policy, scan if feasible, and file in the organization's designated area for storage and/or in the risk assessment document repository.

<Organization Name> <Date of Current Revision> < Your Document #>

NIST 800-53 Safeguard

SESSION TERMINATION AC-12

Control: The information system automatically terminates a user session after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

Assigned Responsibility:< IT Contractor>

NIST Cybersecurity Framework: None in Framework rev 1.0

Suggested Policy Clauses:

1. If idle, the computer system automatically ends a remote session after a <specify> time period chosen by <IT Contractor>.

Review: <annually>.

Implementation Date: _____

Implementing Authority: _____

Authorizing Signature: _____

Revision Date (typically annually): _____

The six Policy Forms covering the 11 safety controls typically used for step 1 are listed below. If other safety controls are in place, additional ACR 2 Cybersecurity Policy Forms are available upon request.

800-171	800-53 Label	NIST 800-53 Title	Form # Pages	Admin/ HR	Local Tech.	Outside Expert	Difficulty*	Revision/ Updating
3.1.1, 3.1.2	AC-2	Account Management	2	X	X		Moderate	Annual
	AC-3	Access Enforcement		X	X			
	AC-17	Remote Access		X	X	X		
3.4.1, 3.4.2	CM-2	Baseline Configuration	2		X	X	Moderate	Annual
	CM-6	Configuration Settings			X	X		Annual
	CM-8	Information System Component Inventory			X			Annual
	CM-8(1)	Component Inventory - Updates During Installations / Removals			X			Annual
3.14.2	SI-3	Malicious Code Protection	2	X	X	X	High	Annual
3.8.9	CP-9	Information System Backup	3		X	X	Low	Annual
3.10.3 3.10.4 3.10.5	PE-3	Physical Access Control	2	X			Low	Annual
3.11.1	RA-3	Risk Assessment	3	X		ACR 2	High	Quarterly

* Difficulty Estimates

Low Difficulty - estimated less than one hour to decide, document, implement and disseminate. Often procedures that exist but lack documentation or formal adoption.

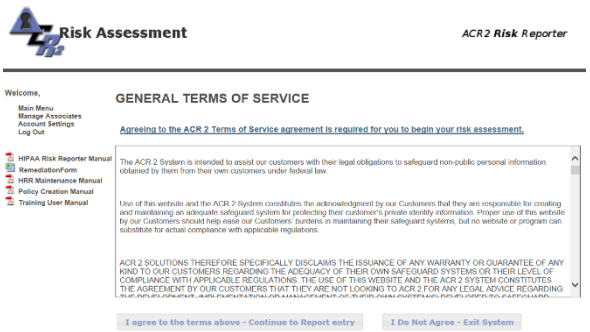
Moderate - estimated less than ten hours to decide, document, implement and disseminate.

High Difficulty - Requires special expertise or tools. May be candidate for outsourcing.

h. Determine and list federally recommended cybersecurity precautions based on protected data type, value and location. A spreadsheet located in the Document Management Center summarizes the NIST guidance in this area for HIPAA, CUI and the NIST Cybersecurity Framework.

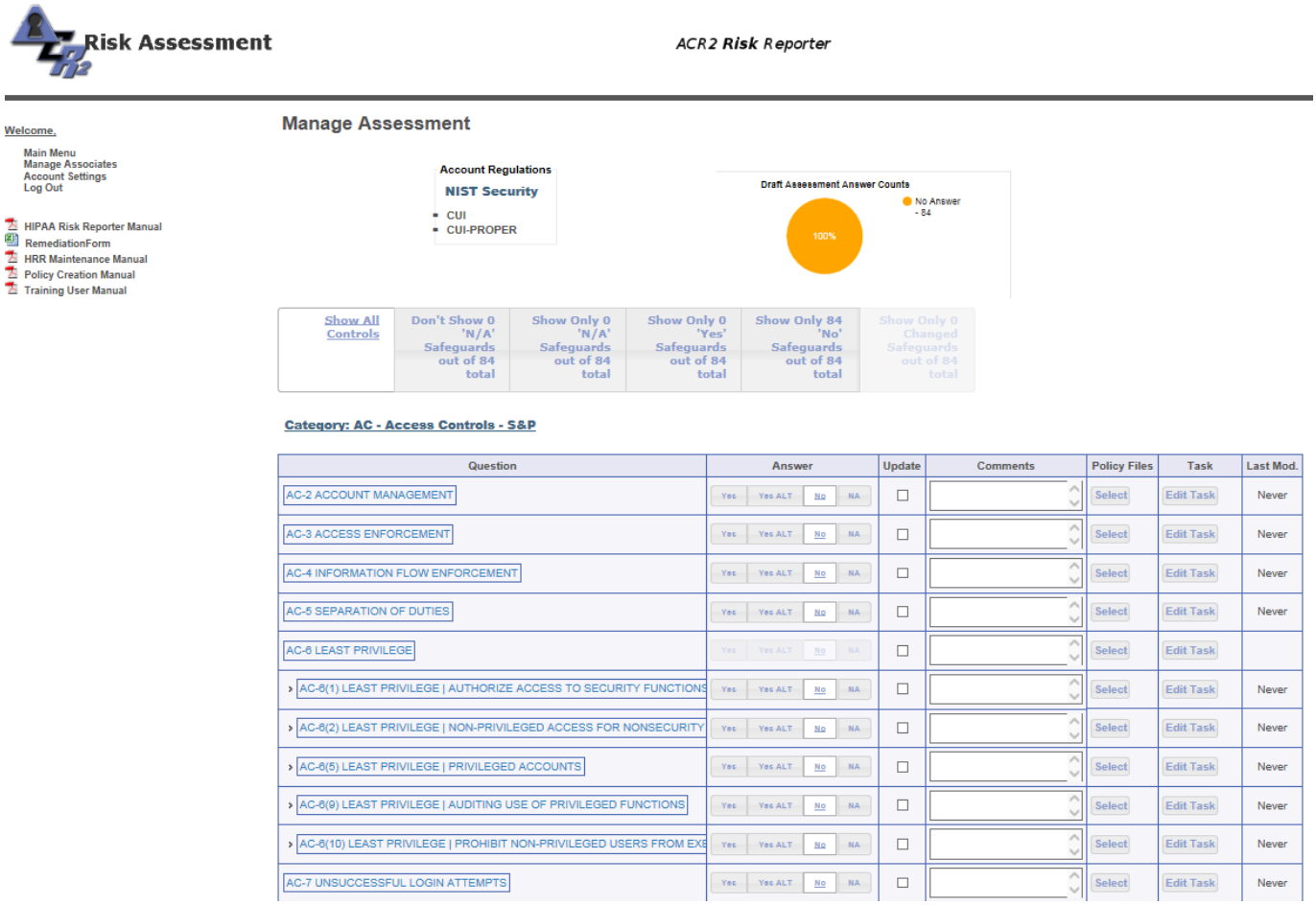
i. Conduct initial risk assessment using the NIST based ACR 2 Risk Assessment software. After logging in, from the main menu click on "Start a New Baseline Assessment"as shown at right. You can save your work and continue again at any time.

j. The next page is the disclaimer and General Terms of Service. In plain language, if your data input is not accurate, the risk assessment will not be valid.



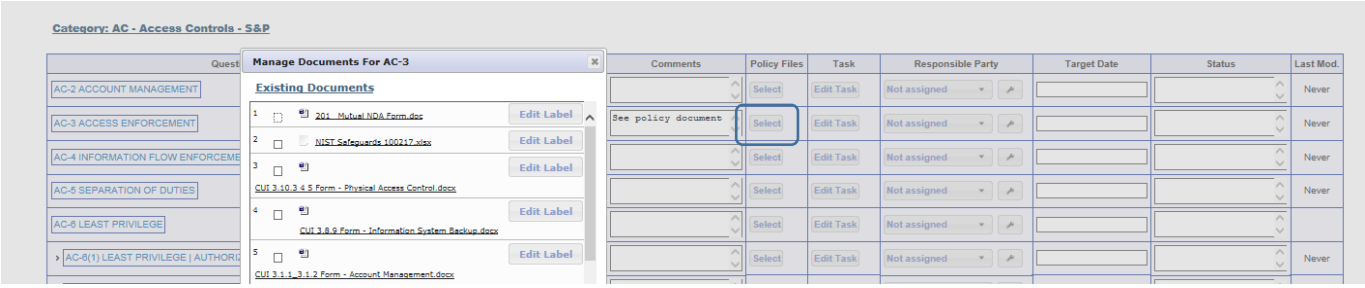
k. Accepting the Terms of Service brings up the data entry page. At the bottom of the data entry page is a "manage assessment" button. Clicking on that button brings up a data entry table that provides a rapid way to do an initial risk assessment. The entire data entry process for step 1 should take less than two hours.

A section of the data entry page for a CUI only site is shown following. Any combination of CUI, HIPAA and Cyber-security Framework sites can be accommodated.

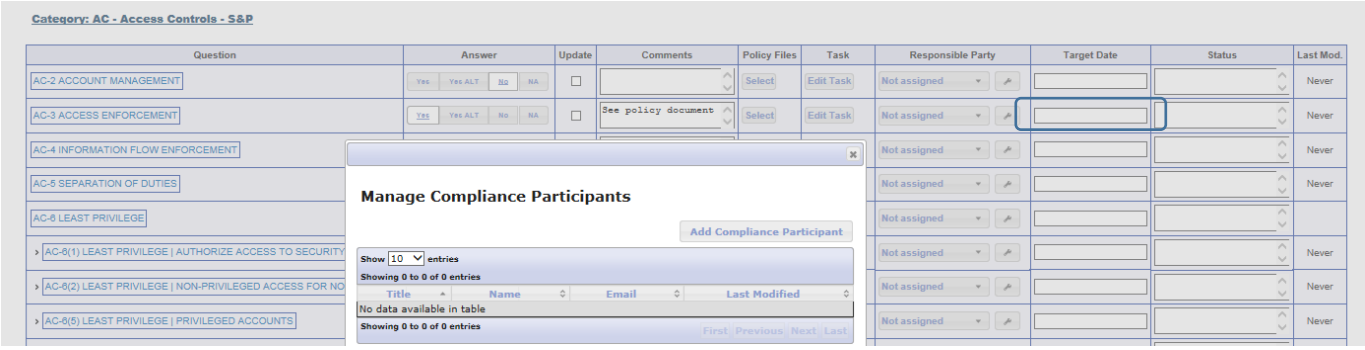


l. There are 84 NIST 800-53 safeguards covering the 109 CUI cybersecurity requirements listed in NIST 800-171. Additional 800-53 safeguards will typically be recommended for HIPAA or Cybersecurity Framework sites. Using your initial signed and dated ACR 2 Cybersecurity Policy Forms, change the NIST 800-53 status for the newly documented safeguards from "No" to "Yes". Note that some cybersecurity requirements such as AC-6 have multiple sub-parts. AC-6 status is not "Yes" unless **ALL** subparts are also "Yes" or "NA", i.e. Not Applicable. NA may occur when a single site organization does not have a multi-site control.

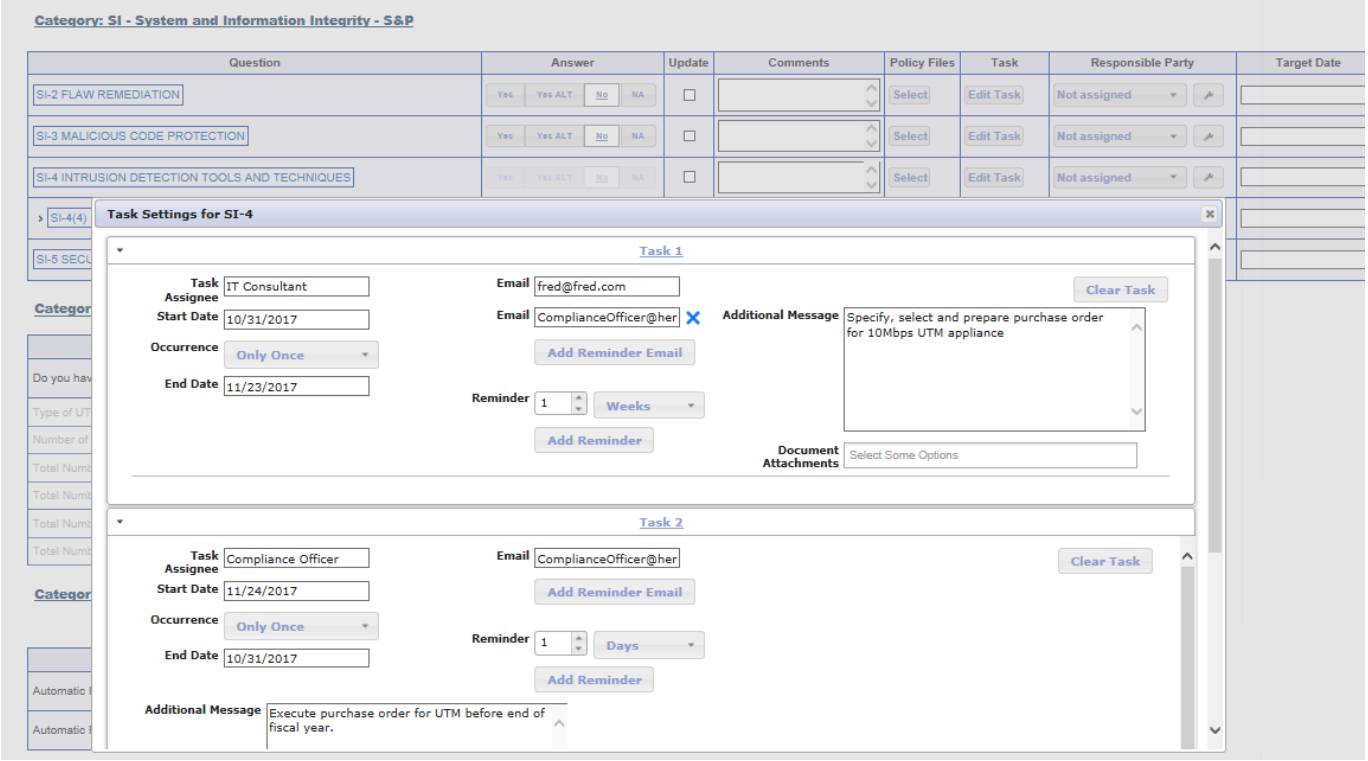
m. For each new "Yes" answer, put "see policy document" in the comments section. The example below shows documenting the AC-3 username and password access control. Clicking on the "Policy Files" button brings up a document management page where 1 or more policy documents can be linked to the safeguard.



n. Clicking on the “Responsible Party” button allows assigning a responsible person for periodic updating, usually annually, of the safeguard. The target date can be assigned by typing in the text box shown.



o. The Task button can be used to assign tasks for updating or implementing new or improved safeguards. In the example shown below, the safeguard SI-4 on Intrusion Detection is partially implemented in two assigned tasks. First, the IT Consultant is tasked to specify a UTM (Unified Threat Management) appliance and prepare a purchase order. Then the Compliance Officer is subsequently tasked with executing the purchase order before the end of the fiscal year. Up to five tasks may be specified for any safeguard.



p. There are 3 parts to the Plan of Action and Miletstones activity. The Gap Report gives a risk weighted listing of missing safety controls in order of overall impact on risk scores. The Gap Remediation Report shows missing safeguards along with assigned responsibilities and scheduled dates of completion. This function is mandatory for medical organizations under the Meaningful Use subsidy program. The Assigned Task Report lists component tasks that are required to implement missing safeguards. Excerpts from these reports are shown on the page following.

Gap Report

Assessment ID:	08-08-16-1470683943
Site URL:	https://www.multiple.riskassess.complianceobjects.com
Finalized date:	Aug 8, 2016 - 12:40 pm
Report date:	Oct 4, 2017 - 1:00 pm

Gap Remediation Report

Assessment ID:	04-20-17-1492724174
Site URL:	https://riskassess.complianceobjects.com
Finalized date:	Not finalized
Report date:	Oct 4, 2017 - 11:08 am

Control	Responsible Party	Target Date	Status
1. CP-2 CONTINGENCY PLAN	COO	Oct 27, 2017	Pending
2. CP-3 CONTINGENCY TRAINING	COO	Not set.	Pending
3. CP-4 CONTINGENCY PLAN TESTING	COO	Not set.	Pending
4. CP-5 CONTINGENCY PLAN UPDATE	COO	Oct 27, 2017	Pending
5. CP-6 ALTERNATE STORAGE SITES	COO	Not set.	Pending

Task Report

Assessment ID:	04-20-17-1492724174
Site URL:	https://riskassess.complianceobjects.com
Finalized date:	Not finalized
Report date:	Oct 4, 2017 - 11:12 am

AC-6 LEAST PRIVILEGE

Task Assignee: Jack Kolh
Start Date: 01/23/2015
Occurrence: Once
End Date: 01/23/2016
Email 1: kolkj@acb2solutions.com
Reminder 1: 1 Weeks
Additional Message: ALERT: In regards to account: u061413-1371238952 (username: CUI template), the remediation date for the control AC-6 is %%target_date%%
Document Attachments:

AC-11 SESSION LOCK

Task Assignee: Jack Kolh
Start Date: 01/23/2015
Occurrence: Once
End Date: 02/28/2015
Email 1: kolkj@acb2solutions.com
Reminder 1: 1 Weeks
Additional Message: ALERT: In regards to account: u061413-1371238952 (username: CUI template), the remediation date for the control AC-11 is %%target_date%%
Document Attachments:

After inputting the data on safeguards status, browse to the bottom of the page, as shown below.

Category: Auto Protection

Question	Answer	Last Mod.
Automatic IPS Protection Enabled	No	Never
Automatic Protection From Viruses Enabled	No	Never

Category: Number With Access

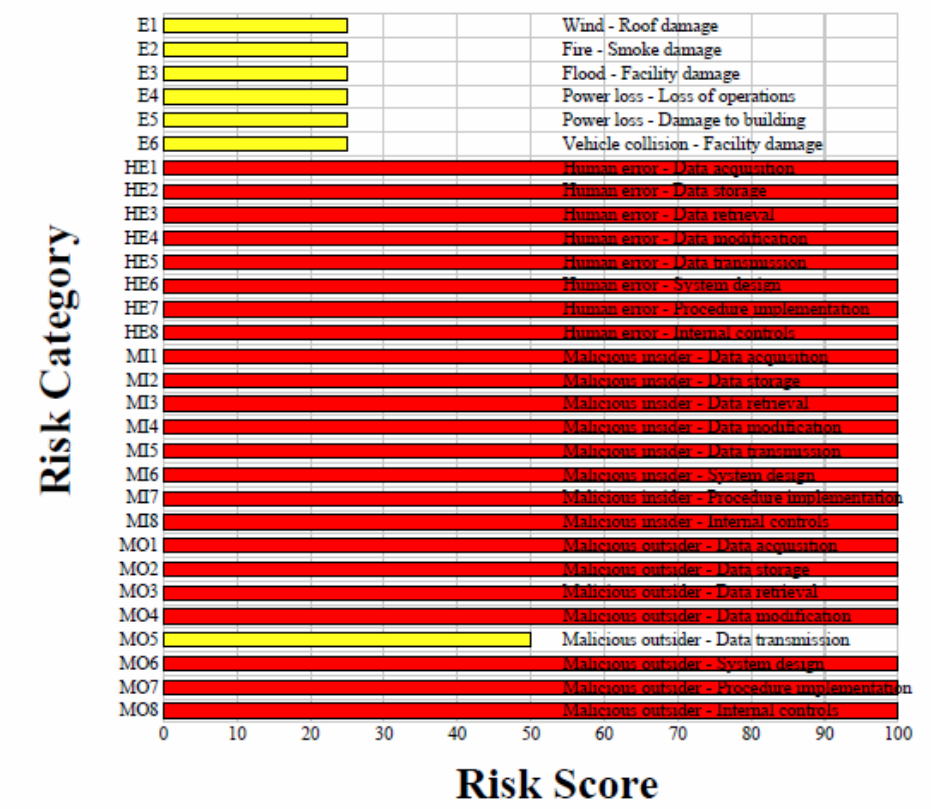
Number of people with access to protected data must not be empty.

Number of people with access and less than one (1) year at this location must not be empty.

Question	Answer	Last Mod.
Total Number of People with Access		Never
Total Number of People with Access and less than one (1) year		Never

q. Input your virus experience and demographic information. If you already have a deep packet inspection firewall or UTM, input that information as well.

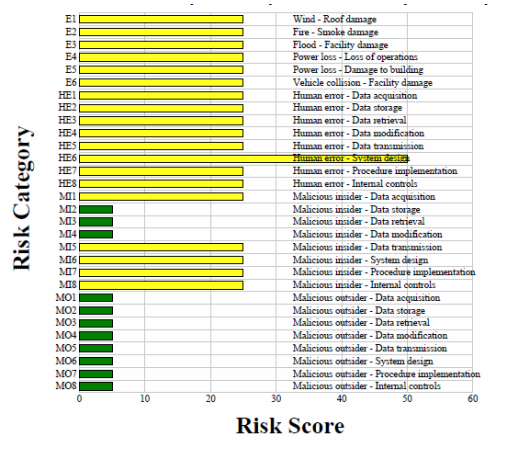
r. At the bottom of the data input page you can select "Submit Answers" if you wish to save your work and come back to it or "Submit and Finalize Answers" if you are ready to generate your initial risk assessment report. Typical initial results are shown below.



Step 2- Implement Basic Cybersecurity Safeguards

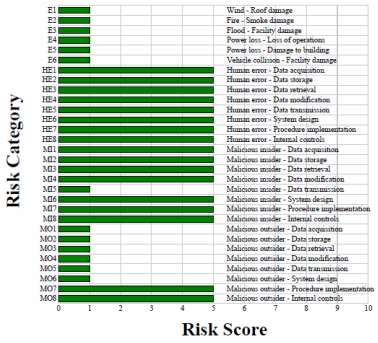
Implement basic list of federally recommended cybersecurity safeguards. ACR 2 Cybersecurity Policy Forms will be provided, typically in batches of 10-15. There are a total of 90 CUI Cybersecurity Policy Forms, with additional Forms for HIPAA or the Cybersecurity Framework. Basic safeguards typically include;

a. Basic personnel policies such as;
   i. Separation of duties
   ii. Initial security awareness training for all users
   iii. Incident response
b. Deep packet inspection (DPI) firewall (Can be provided by ACR 2 partners or locally obtained).
c. Update NIST 800-30 cybersecurity risk assessment. Typical results are shown at right.
d. Generate list of remaining federally recommended cybersecurity precautions



Step 3 – Implement Full Federally Recommended Cybersecurity Program

a) Implement remaining list of federally recommended safeguards, typically including;
   i. Access control policies and procedures.
   ii. Encryption.
   iii. Other safeguards depending on data to be protected, i.e. medical, financial or CUI.

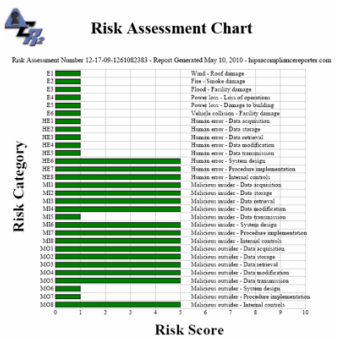


b) Quarterly update of cybersecurity risk assessment. Typical results after safeguards implementation shown at left.

Step 4 – Continue and Maintain Federally Recommended Cybersecurity Safeguards

a) After all federally recommended safeguards in place, update safeguards according to federal recommendations.
b) Annually update cybersecurity training as federally recommended.
c) Annually update cybersecurity risk assessment as federally recommended.
d) Update other safeguards as federally recommended or as conditions and recommended safeguards change. Effects of updating or not updating are shown below.

Updated Account



Same Site Not Updated