Automated Compliance Reporting

Not Just Secure - Compliant!

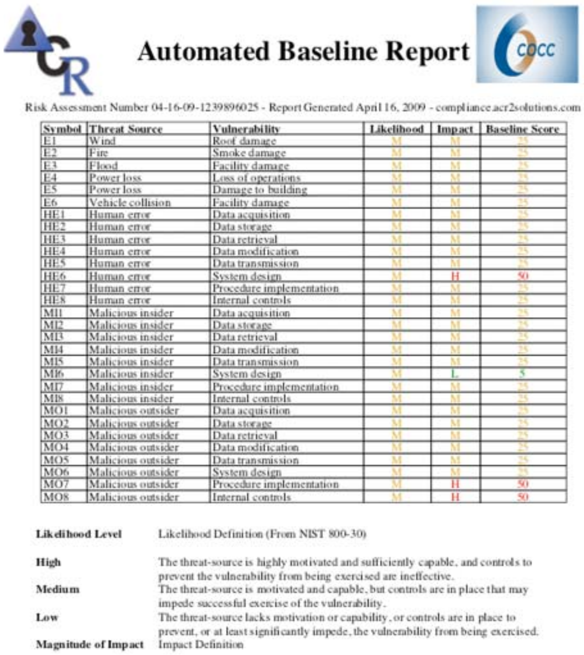
ACR2 Basic - Risk Assessment Software Solutions

Automated Compliance Reporting 2

Automated Compliance Reporting 2 (ACR2) is a family of inter-related software packages that allow automated updating of mandatory **compliance** reports for the twenty million organizations regulated under any combination of the below four regulations:

1. Gramm Leach Bliley Act (GLBA) of 1999
2. Health Insurance Portability and Accountability Act (HIPAA) of 1996
3. Payment Card Industry Data Security Standard (PCI) of 2006
4. The Federal Information Security Management Act (FISMA) of 2002

There is significant confusion about the dividing line between compliance and security. The are related but distinct. Compliance involves meeting the “standard of care” set by whatever regulatory authority oversees an organization. Security is keeping unauthorized persons away from accessing, corrupting or destroying sensitive data.



Automated Baseline Report

Risk Assessment Number 04-16-09-1239896025 - Report Generated April 16, 2009 - compliance.acr2solutions.com

Symbol	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	M	25
HE6	Human error	System design	M	H	50
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	M	25
MI6	Malicious insider	System design	M	L	5
MI7	Malicious insider	Procedure implementation	M	M	25
MI8	Malicious insider	Internal controls	M	M	25
MO1	Malicious outsider	Data acquisition	M	M	25
MO2	Malicious outsider	Data storage	M	M	25
MO3	Malicious outsider	Data retrieval	M	M	25
MO4	Malicious outsider	Data modification	M	M	25
MO5	Malicious outsider	Data transmission	M	M	25
MO6	Malicious outsider	System design	M	M	25
MO7	Malicious outsider	Procedure implementation	M	H	50
MO8	Malicious outsider	Internal controls	M	H	50

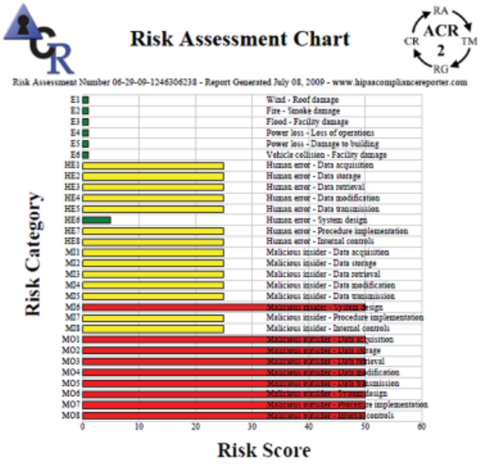
Likelihood Level	Likelihood Definition (From NIST 800-30)
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.
Magnitude of Impact	Impact Definition

What are Organizations Legally Required to Do About Information Security?

More than 20 million organizations worldwide are regulated under GLBA, HIPAA or PCI information security requirements. **None** of these regulations require organizations to be **perfectly secure**. **All** of these regulations require organizations to be **compliant** with similar, specific rules and regulations. There are penalties for non-compliant purchase card (PCI) vendors can be penalized or disqualified from handling credit cards. Enforcement of information security regulations is increasing, driven by significant political pressure and epidemic of identity theft.

For Any Security Compliance Program, Risk Assessment is the Beginning

GLBA, HIPAA and PCI all require regulated companies to perform a **risk assessment** and then take “appropriate” precautions against “reasonably foreseeable” risks. For example quoting from the Gramm Leach Bliley Act (GLBA):

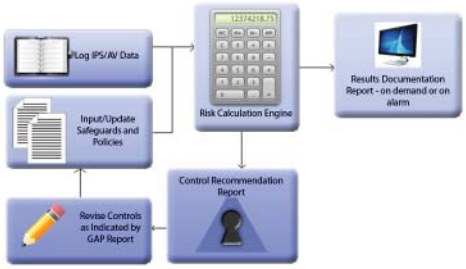


“*Information security program*.. You **shall** develop, implement and maintain a **comprehensive** information security program ... **Appropriate** to your size... Identify **reasonably foreseeable** internal and external risks... and assess the sufficiency of any safeguards in place... At a minimum, such a **risk assessment** should include... (1) Employee training and management; (2) Information systems, including.. (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures... Design and implement information safeguards to control the risks you identify through **risk assessment**, and regularly test..” (**emphasis added**)

For more information visit: www.acr2solutions.com or call 678-261-8181 or email Sales@acr2solutions.com

In the case of HIPAA, GLBA and PCI, there are five common compliance requirements. These regulations require organizations to:

1) perform a risk assessment
2) setup an information security plan
3) install and test the installed safeguards
4) revise the risk assessment accordingly
5) report the test results


Log IPS/AV Data
Input/Update Safeguards and Policies
12374218.75
Risk Calculation Engine
Results Documentation Report - on demand or on alarm
Control Recommendation Report
Revise Controls as Indicated by GAP Report

The process is shown graphically to the right.

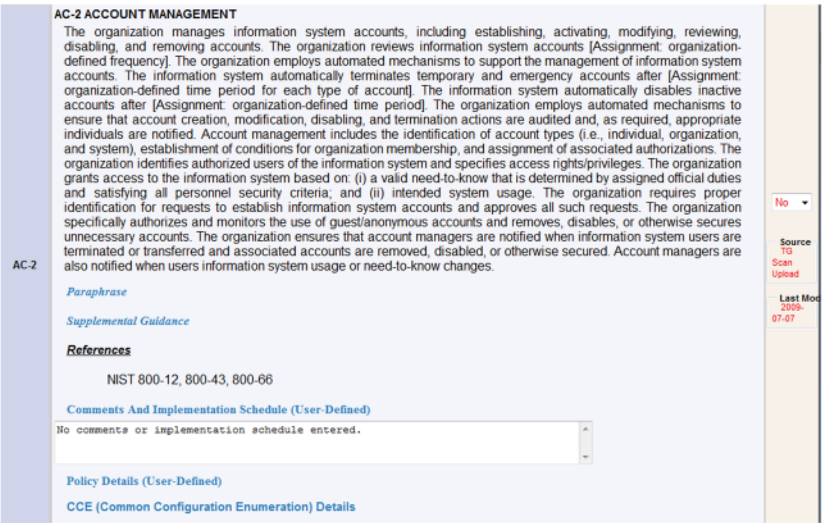
The next step in compliance is to determine how to perform the necessary steps. The National Institute of Standards and Technology (NIST) has published a series of protocols that govern risk assessments and minimum precautions for government systems. These protocols are mandatory for use by the FDIC and other Federal regulators, and recommended for financial and medical companies by such regulators as FFIEC and CMS. The protocols are also long, complex and confusing. For example more than 90 NIST protocols relate to minimum safeguards under FISMA. A single copy of the documents are shown to the left below.

The ACR2 Solution

ACR 2 Solutions, Inc. has created a product that does to compliance regulations what tax programs do to Federal and State tax law. We have converted complex regulations into a straightforward fill-in-the-blank software package. These programs meet the risk assessment and updating tasks required under GLBA, HIAA, and PCI DSS and similar regulations (see items 1, 4, and 5 in the diagram above). Step 2, setting up security programs based on the risk assessment. This is where our included gap report and supplemental guidance can help your IT staff or MSP prioritize. Step 3. Installing and testing safeguards A key element in using ACR2 solutions is that all the safeguards and protocols used by the ACR2 progams are based on Federal recommendations and requirements. The programs reporters have been audited and accepted by the OCC and the FFIEC.

Getting started

To use ACR2Basic just browse to our website and enter your user-id and password and start answering the questions. When you complete the questionnaire press the finalize button. Your encrypted pdf reports are emailed to you. It couldn't be faster or easier!



AC-2

AC-2 ACCOUNT MANAGEMENT

The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [Assignment: organization-defined frequency]. The organization employs automated mechanisms to support the management of information system accounts. The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account]. The information system automatically disables inactive accounts after [Assignment: organization-defined time period]. The organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified. Account management includes the identification of account types (i.e., individual, organization, and system), establishment of conditions for organization membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. The organization ensures that account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users information system usage or need-to-know changes.

Paraphrase

Supplemental Guidance

References

NIST 800-12, 800-43, 800-66

Comments And Implementation Schedule (User-Defined)

```
No comments or implementation schedule entered.
```

Policy Details (User-Defined)

CCE (Common Configuration Enumeration) Details

No

Source
TG
Scan
Upload

Last Mod
2009-
07-07

ACR2 Solutions
How Much Is Your Time Worth?

For more information visit: www.acr2solutions.com or call 678-261-8181 or email Sales@acr2solutions.com