

# Risk Assessment Without Pain

By Caroline Hamilton & Mary Brandt

**Some healthcare professionals dread the task of planning and conducting the HIPAA-required security risk assessment and gap analysis, but with good support and the right tools, the job is very manageable and will pay big dividends for the whole organization.**

Risk assessment is the cornerstone of any information security program, and it is the fastest way to gain a complete understanding of a healthcare organization's security profile – its strengths and weaknesses, its vulnerabilities and exposures.

The security regulations proposed under the Health Insurance Portability and Accountability Act (HIPAA) require regular risk assessments and gap analyses to assess the overall organizational security. Many healthcare organizations are nervous about beginning such a high profile project, but there are tools you can use which will not only reduce anxiety, but take away the pain altogether.

If you've been selected to manage the security risk assessment project, your first task is to determine the scope of the effort. Should it include the entire organization's data processing components, only the networks, or just the key databases? Do you have to include every single PC and network connection? How do you calculate the value of patient information? Should you use an automated package? Which one? Should you hire an outside consulting company to help, or should you let them do the whole thing?

Most important, what results should you expect, and how can you convey these results to management in a meaningful way? This last question is a key consideration. A short, concise report is much more valuable than a lengthy report which contains a jumble of confusing numbers and no specific recommendations. To gain the support of senior management, you'll need to give them a clear picture of your critical and sensitive assets, with detailed information on which ones are most in need of protection and how they should be protected.

## Requirements for risk assessment are increasing

Reacting to widespread media coverage of computer incidents, Congress passed The Computer Security Act of 1987, thereby launching managers into a new era of accountability. The Office of Management and Budget (OMB) had previously set requirements for risk assessment in OMB Circulars A-71, A-123, and A-130. In addition, the Defense Department recently created the DITSCAP (Defense Information Technology Systems Certification and Accreditation Process (DoD 5200.40) variety of other unique requirements mandating risk assessment. The most common requirement is that organizations should conduct a risk assessment every one or two years, or any time there is a major change to the information systems. While the proposed HIPAA security regulations do not yet specify how often a risk assessment should be conducted, it makes sense to follow the federal guidelines.

## What is risk assessment?

A risk assessment can be called by many names: risk assessment, management review, gap analysis, risk management, vulnerability assessment, loss prevention, review of a sensitive application, or security audit. Each name refers to the same function—analyzing an information system, an organization, a physical facility, or a business process, in order to assess its existing security profile, and to identify the safeguards needed to bring the system's security up to the desired level. A risk assessment also provides a means of analyzing all potential threats to an organization, as well as their likelihood of occurrence.

Risk assessment gives you a clear picture of your loss potential. It establishes expected losses from defined threats based on asset exposures, vulnerabilities, and estimated probabilities of occurrence. It identifies the problems you could expect to encounter with your information systems or facilities, whether that includes managing sensitive patient databases, making sure that physical controls are in place, and

limiting access to information to individuals who need that access to do their jobs.

A risk assessment analyzes the relationship between five critical components:

**Assets** – The resources the organization wants to protect, including computers, networks, applications, databases, hardware, software, facilities, and personnel.

**Threats** – The potential events that could cause harm to the system or generate losses. Examples: unauthorized access to sensitive patient information, altering financial records, fraud, embezzlement, worms and viruses, catastrophic fires, and natural disasters.

**Vulnerabilities** – The “windows of opportunity” which could allow a threat to materialize. For example, the lack of a fire-detection system can allow a fire to get out of control.

**Losses** – Anything that can be taken away from the organization. This includes loss of data integrity through modification, or destruction, theft of equipment, delays or denials of service, or even loss of life.

**Safeguards** – Administrative, physical, or technical controls designed to provide protection and reduce vulnerability. Examples of safeguards could include cipher locks and terminals that log-off automatically, biometric devices for user authentication, doing background checks on personnel, and having an emergency response plan.

## The “classic” method

In the traditional method of risk assessment, a questionnaire is used to survey users and determine whether the existing controls and standards are actually in use. Ask a security manager whether a password program is in place and whether all users are complying, and you will usually get an affirmative answer. However, if you ask 60 system users individually if they are using their passwords, you will generally find something quite different. You may also find that one group of users doesn't turn their computers off when they go to lunch because they don't want to have to log-on again. A new employee's background check hasn't been

finished, so the supervisor lends him a password until the check is complete. Many users have their “secret” passwords (yes – their pet's name) stuck on a Post-it™ note above their terminals.

## Manual methods too slow and cumbersome

One reason managers have been reluctant to start risk assessments is that conducting a manual risk assessment can be very expensive, in both time and dollars. The cost of a manual risk assessment for a large, complex network is huge, and the assessment may require months to complete. Indeed, the time factor involved in reviewing the many components in large systems has rendered many risk analyses obsolete by the time the final report is written.

The difficulty of the risk assessment process increases exponentially with the complexity of the system under review. When considering a single computer, it is certainly feasible to do a manual risk assessment, even though the cost may be high. However, when the system under review includes over 800 microcomputers, interconnected with several mainframes spread over a geographic area of several thousand miles, manual assessment becomes virtually impossible. Aside from the combinatorial problems, expertise in both risk assessment and computer security is needed to draw valid conclusions from the voluminous data that must be collected.

## Automating the process

Automating the risk assessment process is a major improvement over doing it manually. Just ask Lesley Berkeyheiser, a healthcare consultant specializing in HIPAA compliance and principal in The Clayton Group, and National Co-chair of the WEDi-SNIP security and privacy subgroup. She has assisted several healthcare organizations in beginning the process of HIPAA compliance and has done assessments both with and without tools. *“Without the help of software, it's a very cumbersome task. It's not impossible, but it would take months just to complete the gap analysis portion of the HIPAA regulations, much less complete the risk assessment, not to mention the volumes of paper involved. I often tell people that using tools like HIPAA-Watch, allows*

*a covered entity to make scalable and reasonable business decisions. With a fully automated program (like HIPAA-Watch), you can do it three times faster, and the results are much more accurate.”*

Automating the security risk assessment required for HIPAA has some key advantages over the manual process:

1. The level of effort is greatly reduced, often by 50 percent or more.
2. Major cost savings can be realized on subsequent analyses when systems have to be recertified.
3. Automation makes it easier to consider the effects of different safeguards. It allows you to play “What if?” to help develop the best level of protection for the least cost.
4. Automated packages are adaptable to many environments, even new systems or new facilities being developed.
5. Many automated packages can produce both quantitative and qualitative results.
6. Updated data can be easily added at any point of the assessment.

## Selecting an automated risk assessment package for HIPAA

Ten years ago, few security risk assessment packages were available, and they were generally cumbersome, based on spreadsheets, and difficult to use. In recent years, however, several PC-based risk assessment packages have been developed and marketed. These packages automate many of the labor-intensive tasks involved in a security risk assessment. Automated methodologies generally provide either quantitative or qualitative results; a few can do both.

Very few risk assessment programs are suited to doing the gap analysis and risk assessments required for HIPAA. The newness of the content and the difficulty some programs have in updating has limited the availability of these programs.

In evaluating automated tools, such as the HIPAA-Watch product, by RiskWatch, consider the guidelines provided in the National Institute of Standards and Technology (NIST) Special Publication 500-174, *Guide for Selecting Automated Risk Assessment Tools*. It recommends that packages include three fundamental components:

**Data Collection.** The method used to compile asset information, data on the operational environment of the system under review, as well as collection of questionnaire data from assessment participants.

**Data Assessment.** Techniques can include statistical methods, sampling techniques, the Delphi process, Monte Carlo modeling, regression analysis, and use of expert systems.

**Report Generation.** The form taken by the output data from the risk assessment, how the report is configured, whether it can be tailored to individual needs, and whether the report includes graphics.

In addition, you will probably want to consider the following factors:

**Program Operation.** Does the methodology meet existing risk assessment guidelines? Has it been tested in a regulatory environment so you can be SURE it meets federal requirements? Does it comply with a methodology that has already been endorsed by your agency or organization?

**Compliance with Requirements.** Does the program include the exact regulatory requirements? Does it include gap analysis to measure compliance with Privacy regulations and the administrative, technical and physical requirements of HIPAA?

**Ease of use.** Is the program easily installed and implemented without needing a consultant?

**Tailoring.** Can the program be easily tailored so that its screens reflect your organizational environment?

**Question Development.** Does the program allow you to create your own questions, and to modify existing questions and standards?

**Questionnaire Distribution.** Can questionnaires be distributed to survey recipients by e-mail, diskette, or over a network, to both end-users and administrative

and medical personnel? Can questions be answered, and returned on disk or via network, and automatically uploaded?

**Legal Review.** Have the program and its standards undergone a complete legal review by a law firm that specializes in HIPAA compliance issues?

**Report Generation.** Does the program write the report automatically? Can be easily changed and adjusted by the user?

**Usefulness to Management.** Are graphics easy to understand? Is the report written in non-technical, easy-to-understand language?

**Vendor Support.** What support does the vendor provide training in the use of the package? Is there a mechanism to keep users informed of product enhancements? Is telephone support provided at no additional charge?

**Updates and Enhancement.** Is the product upgraded by a major release at least annually, or whenever the regulations change?

**Cost.** Is the cost reasonable when balanced against the performance and output of the product?

## Risk assessment is good management

Many healthcare managers face gap analysis and risk assessment with a groan, seeing only a complicated project without any redeeming features. Risk assessment as a management tool is actually a vital element in the overall management of patient records, medical records, or any information system.. Because of the different interpretations of the term “risk management”, there has been a great deal of confusion about risk assessment/risk management. This accounts for the reluctance of many healthcare managers to incorporate gap analysis risk assessment into their HIPAA toolbox. The U.S. General Accounting Office (GAO) recently reported on using risk assessment to deal with biological terrorism, and said, “We have previously reported on the value of a new, approach of using sound threat and risk assessments for focusing programs and investments to combat terrorism. Without such assessments, there

is little or not assurance that programs and spending are focused in the right areas in the right amounts.”

## The future of risk assessment

Commenting on the future of risk assessment in the HIPAA environment, Gary Swindon, former Chief Security and Privacy Officer for WebMD and security industry advisor said, *“Any program that seeks to achieve HIPAA compliance must have an enduring quality since, by it’s very definition, HIPAA is forever. Nowhere is a solid risk management program more important – just as HIPAA will endure, risks will change with time and efforts to contain them, forcing the risk management effort to take on similar ‘enduring’ qualities in order to be of value to the company.”*

With requirements increasing as fast as the losses, the final question remaining for HIPAA managers to think about security risk assessment is not whether they have to do it, or can afford to do it, but whether they can afford *not* to do it.

Caroline R. Hamilton is a free-lance writer and President of RiskWatch, Inc., a private company specializing in security risk assessment software. Mary Brandt is President of Brandt & Associates, Inc., a national healthcare consulting firm that provides HIPAA consulting services to a wide range of clients.