

# Risk Assessment: Where Security Meets Compliance

## A Guide on How to Structure and Manage the Risk Assessment Required by the new Joint Commission Standard.

By Caroline Hamilton and Peter Ochinko

### INTRODUCTION TO RISK ASSESSMENT

The Joint Commission issued a new requirement for hospitals in October of 2007. It primarily affects the physical security of hospitals, with particular focus on the neonatal unit, visitor access to particular areas of the hospitals, including the emergency room.

The first requirement in this new standard is: “*Conduct an annual Risk Assessment that evaluates the potential adverse impact of the external environment on the security of patients, staff, and others coming into the facility.*” The second requirement is: “*Use the risks identified to select and implement procedures and controls to achieve the lowest potential for adverse impact on security.*”

Other areas of the standard address whether staff wear badges, how visitor access to the neo-natal is handled, how new babies should be tagged, whether the organization has a program in place to mitigate violence in the emergency room, and other related areas.

How to conduct, deploy and manage a large risk assessment is a very complicated process, and the understanding of how to map identified risks into effective controls is the focus of this article.

Risk assessment is the foundation of any security program. Whether it is analyzing security of a large distributed campus of dozens of building, or whether it is analyzing a single free-standing hospital, it is a standardized way of addressing and managing risk. Risk assessments look at a variety of threat scenarios, reviewing the value of the organization’s assets (which includes the well-being of the patients), and using quantitative data (measurable information), to develop a risk factor and also solutions that afford the organization protection against the most likely risks, and the solutions are then evaluated by their cost-effectiveness – or ‘**The Best Bang for the Buck**’.

## **What Is Risk Assessment compared to a Site Survey ?**

• A process used to determine what controls are needed to protect critical or sensitive assets adequately and cost-effectively.

The process examines five kinds of information:

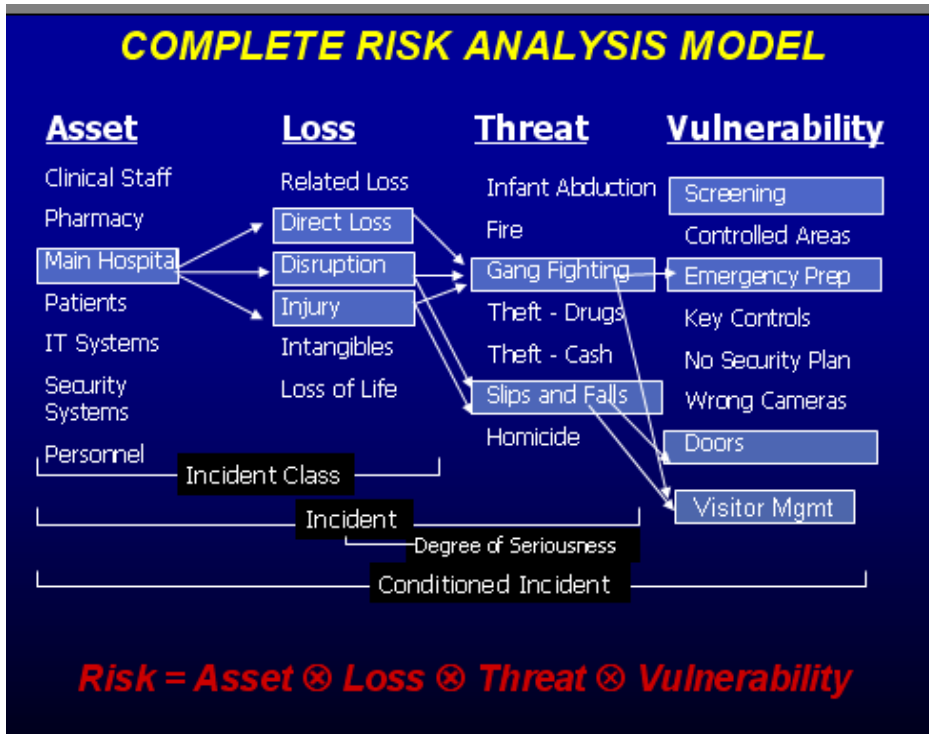
1. Specific Assets to be Protected (value)
2. Potential Threats to the Assets
3. Vulnerabilities that would allow the threats to materialize
4. Kinds of Losses that the threats could cause
5. Controls that would reduce the loss or eliminate the threats

A Risk Assessment, by definition, must include the following elements:

1. **The Assets that Need to be Protected** – for example, Patients, Staff, Pharmaceuticals
2. **The Threats that Might Occur** – Theft, Vandalism, Violence
3. **The Vulnerabilities in the Organization** that would leave a ‘window of opportunity’ allowing the threat to materialize – e.g., not having a visitor management program, not using staff badges, leaving doors unlocked in a sensitive area.
4. **The potential losses** the organization would sustain if the threat occurs - infant is stolen, patient dies on emergency room floor.
5. **The Controls** which would either reduce the impact of a threat occurrence, or eliminate the possibility of the threat materializing. Having each infant banded, not printing birth notices, having a current visitor management system.

Each element is then analyzed against every other element to create a risk assessment. First, the Assets are linked to Potential Losses, then the relevant threats are examined to see what threats are a higher likelihood of occurrence in this environment. Security vulnerabilities identified in the compliance survey are added to the model. Lastly, potential controls are analyzed to see which controls would offer the protection needed, and are then ranked by Return On Investment.

Here’s an example of how each category is mapped to every other category:



### MOVING PHYSICAL SECURITY UP TO THE C-LEVEL

The effect of the new Joint Commission requirement is to elevate the physical security program up to a higher level in the organization. It integrates the security function into the management of the organization, primarily because security is now a major element in an organization's ability to carry out its primary function – providing health care. Having a risk assessment requirement also impacts the security budget. Because compliance is the driver – it may be easier to get management buy-in to improve security in the hospital. This includes answering questions like: how much security do we need to be secure? How much does it cost to improve our security program to the most effective level? And, for the first time, are we, as an organization compliant with the new security guideline?

#### **Risk assessment is a management process and should involve all areas of in the hospital.**

Employees must be an integral part of the risk assessment process. Employees see security from a different and very valuable perspective -- they integrate it into their daily work. Whether you are going to include admissions staff, clinical staff or security officers, getting information from a wide variety of individuals is extremely important to the validity and accuracy of the risk assessment.

In order to make it easy to involve others in the organization, management involvement from the very beginning can make the difference between a successful risk assessment and one that is difficult to complete, with the final results possibly questioned or

disregarded. The key to obtaining strong organizational support for the risk assessment includes the following elements:

- Getting Management Buy-In
- Involving the Entire Organization
- Asking Good Questions - Developing a Survey Method
- Structuring an Effective Project Plan

### **Management Buy-in for the Risk Assessment**

If you are conducting a risk assessment, it means that the activity AND the budget for risk assessment have already been approved by management, whether you have your own in-house staff, or are using an automated software program or an outside consultants, or some combination of all three. Just having the go ahead for a risk assessment is not enough. You will need management support from the top of the organization to be able to do an effective assessment.

### **Asking Good Questions – The Compliance Surveys**

Asking good questions is the very heart of the risk assessment. Questions should be set up to validate compliance against published policies, guidelines and directives (for example, the Joint Commission or Environment of Care standard, or the IAHS standard). If you ask questions that are not linked to standards, and discover major problems, the path will not exist to force compliance. Limiting the number of questions to ask is one of the most difficult aspects of the analysis.

It is unrealistic to think that people will answer more than fifty to one hundred questions. To avoid individuals having to answer questions that do not relate to their area, in a risk assessment, questions are divided into job categories, or what is called 'functional areas.' Functional areas are pieces of a job. By dividing up questions into these categories, for example, Michael Smith may answer 10 general questions, 20 questions for clinical staff (which is his area), and 15 specific questions about visitor management. More specialized personnel, such as facilities managers, the physical plant manager, or an administrator will answer questions that relate only to his/her particular area.

Questions should be mapped together so management can easily see who answered the questions and how many of the individuals reported a particular finding (see chart below):

<b>RESPONDENT</b>	<b>Non Compliant</b>	<b>Compliant</b>	<b>NotApplicable</b>	<b>Don't Know</b>	<b>Compliance</b>
Bill Smith	124	49	9	36	28%
Ron Lee	110	12	1	24	10%
Deb White	97	24	12	22	20%
Dave Hall	49	70	1	74	59%
Mark Smith	47	137	8	22	74%
Jane Gibbs	43	37	0	46	46%
Barb White	43	78	102	10	64%
Rochelle Ramsey	35	57	21	16	62%
Glenn Johnson	0	1	0	0	100%
Allan Brown	0	2	3	0	100%

### **THE ACTUAL ANALYSIS PROCESS**

The most difficult part of a risk assessment is the actual analysis. There can be more than five million potential combinations of just 25 asset categories, 38 threat categories, 7 loss categories, 40 vulnerability categories and 200 potential safeguards (controls). So the analytics involved in analyzing the collected information is a major element of the assessment and those analytics are used to produce the final report.

A report should include:

- Asset information
- Threat matrixes
- Compliance and vulnerability graphs (see below)
- The loss impact projections
- And the controls recommended by their Return On Investment.

The following example shows what you need to include in a threat evaluation:

LAFE = Local annual Frequency Estimate – How often the threat has occurred in your environment.

SAFE = Standard Annual Frequency Estimate – How often the threat has occurred on average in other similar organizations.

THREATS	CURRENT	UPDATED
	LAFE	SAFE
Accident	0.02	0.20
Activist/Riot/Civil Disorder	0.10	0.10
Arson	0.02	0.05
Assault	1.00	1.00
Blackmail/Extortion	0.05	0.05
Bomb Threats	2.00	0.10
Burglary/Break In	1.00	0.50
Communications Failure	6.00	6.00
Data Disclosure	3.00	5.00
Earthquake	0.05	0.05
Explosion, Major	0.01	0.01
Explosion, Minor/Mail Bomb	0.10	0.10
Flooding/Water Damage	0.05	0.10
Fraud/Embezzlement	1.00	1.00

Available sources of threat data can include the organization's own Incident Reports, local police statistics, the American Hospital Association (AHA); the National Oceanographic and Atmospheric Administration (NOAA), FBI Crime Statistics, National Fire Prevention Association (NFPA), Bureau of Transportation Statistics, the Disaster Recovery Journal, the National Institutes of Health (NIH), the Centers for Disaster Control and Prevention (CDC) and many other diverse sources.

The analysis should include cost benefit information, so that controls are ranked by how effective they would be in reducing the identified threats.

A cost benefit analysis report combines information from:

- a. the vulnerability assessment
- b. the relevant threat data and asset information such as present day replacement values and criticality
- c. and how completely safeguards are currently being implemented, and how much they would cost to fully implement.

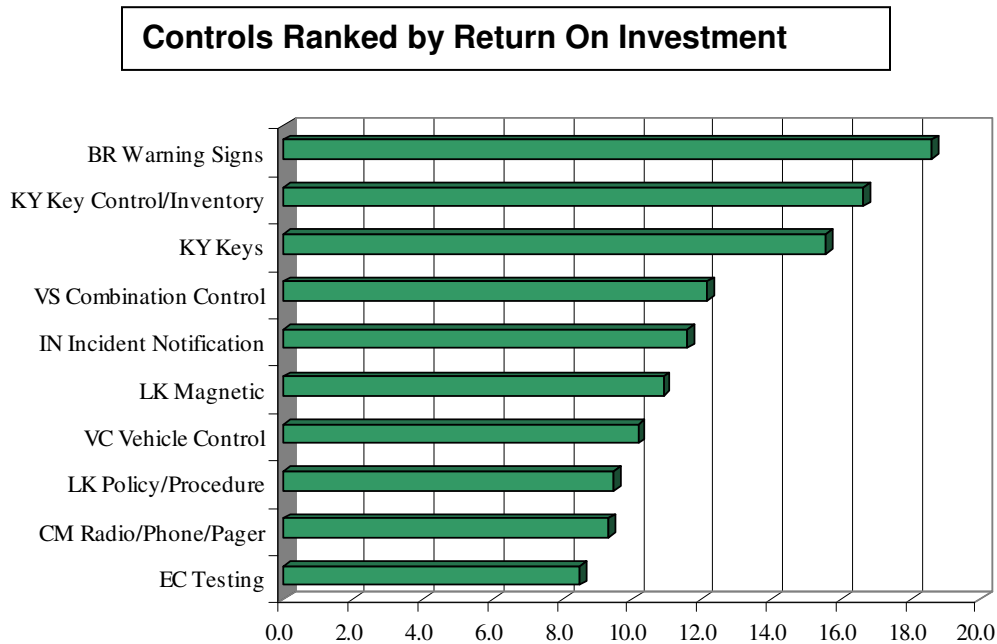
In reviewing the existing security controls, it's important to indicate percentages of current implementation. For example, maybe the visitor badging policy is only 70% implemented, meaning that it is implemented on weekdays, but not on weekends.

In actual risk assessments, completing implementation of an existing control to 100% is often the most cost effective solution. The result of the cost benefit analysis would be to create a return on investment ratio (ROI), balancing the value of the information against the cost of controls to protect it. By establishing Return On Investment data, managers

and directors can make more informed decisions regarding which controls to implement, based strictly on initial cost, but also on the current threat exposure of the organization.

The graph below demonstrates what a Return On Investment would look like. The potential controls are analyzed by:

1. The percentage of the control currently in place.
2. Whether it is a “critical” control?
3. How much it costs to implement the control completely.
4. How much the Control mitigates each individual threat.



The annual risk assessment can be a standardized way to improve security over time and at the same time, meet the current requirements of the Joint Commission. While management support is critical, it will elevate security to a higher level inside the organization and make it easier to budget critical security improvements.

## **Caroline R. Hamilton**

410-224-4773 x105 – o  
301-346-9055 – c

[chamilton@riskwatch.com](mailto:chamilton@riskwatch.com)

Caroline R. Hamilton is an expert in security risk analysis and security risk assessment and President of RiskWatch, Inc., a company specializing in security risk assessment software. She was a Charter member of the National Institute of Standards and Technology's Risk Management Model Builders Workshop, which was a joint Workshop between U.S., Canada and the United Kingdom to create the first security risk management guidelines from 1988 – 1995. In 1996, she served on the U.S. National Security Agency's Network Rating Model workshop, and from 1996-1998, served on the working group to create a Defensive Information Warfare Risk Management Model, for the U.S. Department of Defense, under the auspices of the Office of the Secretary of Defense.

Hamilton has been working in a variety of industries to develop automated security risk assessment models and programs, including the healthcare, financial, critical infrastructure, and the maritime and defense industries. Hamilton has worked with the U.S. Department of Justice to create security vulnerability assessment guidelines for the U.S. Homeland Security Infrastructure Protection initiatives and risk related to Critical Infrastructure Protection.

She is currently developing custom risk assessment models for hospital security to meet the Joint Commission requirements, and is a member of the IBM Data Governance Council, and the ASIS Information Security and Technology Council. She is a graduate of the University of California, Riverside and lives near Annapolis, Maryland.

## **Peter Ochinko**

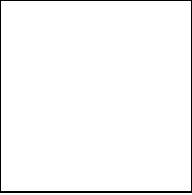
954-467-3964 – o

954-445-2461

[pochinko@iaccsys.com](mailto:pochinko@iaccsys.com)

Pete Ochinko spent over 20 years with the United States Secret Service. Upon his retirement in 2002, Peter accepted a position with Memorial Healthcare System, a six hospital system in south Florida, as Corporate Director of Security. During his tenure as Director, Pete implemented one of the most comprehensive security plans in the hospital industry. As a result of his ground breaking work in the industry, he was awarded the prestigious Lindberg Bell award from the International Association of Hospital Safety and Security for excellence in the field of hospital security.

Pete is now the President of Integrated Access Systems (IAS), a security company specializing in the design and implementation of comprehensive security and training programs for hospitals, schools and large corporations.



In his new role as President of IAS, Pete now works with a variety of hospitals, schools and corporations developing comprehensive security and training programs for various clients across a broad spectrum of industries and applications, combining his background in security, access control and healthcare systems. Pete is a family man, and is very active in the lives of his wife and three children in south Florida.