Risk Assessment, Say What?

John R. Bennett, PEM
Hospital Network Healthcare Service
Portage, Michigan – July 2009

You have just been given the job of doing a risk assessment for your organization. You have heard of a risk assessment but never had to do one. You are asking yourself, "What do I need and where do I start?"

According to Disaster Recovery Journal (www.drj.org) a risk assessment is the *"process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls."*

A risk assessment is an ongoing process that is living and breathing and is a strong part of an overall risk management program. The risk assessment is an early and important step in the development of business continuity plans, disaster recovery plans, emergency action plans, etc. Without this process of discovery, these plans will not be properly developed and gaps will occur which could lead to loss of revenue, fines, production downtime, and/or loss of lives. You must know what your vulnerabilities are and what is being done, or if nothing is, what can be done to eliminate or minimize these vulnerabilities.

If you conduct an internet search on risk assessment you get approximately 27,000,000 responses. Where do you start with this seemingly daunting task? You can break it up into four main stages using the PADS process (Planning, Assessment, Documentation, and Submission), with the first stage being **planning**. The **planning** stage is a preparatory stage in which you will organize the task and set up what you are going to do and how you are going to do it. There are several things you are going to want to look for during this stage:

- ✓ Is management supporting this project?
- ✓ Is funding available?
- ✓ Are other people available to assist in data collection?
- ✓ What areas or tasks are being assessed?
- ✓ Who are the key stakeholders for those areas?
- ✓ Is your assessment going to be quantitative, qualitative, or a combination?

Having a team involved in the assessment process is very beneficial and can lead to a better and more thorough risk assessment. It is best to have people who are knowledgeable in the process or areas that are being assessed. Through the team, different views are offered and it follows "two heads are better than one."

Set the scope for the assessment and the objectives and make sure your team is on board with this. Establish your goal(s) that are needed in order to meet the final objective(s). Plan your assessment and set up a schedule. Write out what you are going to do, who is going to do what, and when it needs to be done.

The second PADS stage is the actual act of doing the **assessment**. This could be called doing the field work or collecting the data. In this stage you and your team members are going to collect information keeping the agreed upon goals and schedule in mind. Some of the things you might be doing during this stage are:

- ✓ Coordinating the time(s) with management.
- ✓ Identifying the hazards and what is at risk.
- ✓ Assessing risks that are possible due to hazards.
- ✓ Running collection/evaluation tools if needed.
- ✓ Evaluating or recording any preventative measures in place and their effectiveness.
- ✓ Determining best preventative action(s).

You definitely want to work with the managers and supervisors in the area you are doing the assessment. They can give you the best times to do your assessment and lead you to the subject matter experts to assist you in getting the most reliable information.

Collecting and identifying hazards is a large task in itself. Hazards can be natural, such as a tornado, ice storm, influenza, flood, lightning, wild fire, etc. Other hazards can be man-made such as a terrorist attack, civil unrest, or even technical such as a hard drive crash, server failure, computer virus or worm, or something as simple as someone pulling the wrong plug. You want to review these and then look at what is in place to mitigate, or remove, the potential issues the hazard can cause, or at the least lessen the severity. One example of this would be using anti-virus software to protect computer systems from viruses.

Now we are at the third stage of our risk assessment. This is **documentation**. You will want to collect all of the team's findings and put them in a logical and usable format for submission or presentation to the person(s) requesting this be done. This information is also used in the next phases of a plan such as the business impact analysis phase of business continuity planning.

Another reason you want to record this information is possibly for regulatory requirements such as those found in the Health Insurance Portability and Accountability Act (HIPAA) which requires a risk analysis be completed. What do you want to show in your documentation? You will want to cover the following:

- ✓ What potential hazards were found?
- ✓ What are the potential risks of the hazard?
- ✓ What were the safeguards in place for each hazard and are they adequate?
- ✓ Are there better safeguards than those being used?

For your **documentation** you should keep things together and organized. Tie the risk to the hazard and then the safeguards. Then you can add in other recommendations that the team has come up for that particular risk. You can then weigh them and put them in some order such as by the risk that poses the greatest potential for loss to the least.

This is all done in order to do the final stage which is the **submission** of the finding and recommendations. This submission can be in the form of a written report, a presentation, or a combination of the two.

Here are a couple of things to keep in mind throughout the **PADS** process and in particular for the submission:

A. It is always easier to get the best safeguards if you use quantitative assessments as opposed to qualitative. It is easier to see the loss in a dollar figure, such as $50,000 per day when a particular machine is down, than it is to just say that it would cost us a lot of money to have this particular machine down.
B. When possible, give your recommendations for safeguards in levels such as gold, silver, and bronze. This way management can evaluate the potential risk against the expense. They may decide against any of your team's recommendations but you will have given them the best tools for them to make their determination.

A risk assessment may be a long process and take a great amount of time to do but the outcome is very important to the organization. What this may find may save a life.

Remember the four steps of the **PADS** process of risk assessment are:

1. Planning
2. Assessment
3. Documentation
4. Submission

Here are a few websites on business continuity, disaster recovery, and emergency management.

Disaster Recovery Institutes International (www.drii.org).
Disaster Recovery Journal (www.drj.com)
FEMA (www.fema.gov)