WHAT IS THIS THING CALLED RISK MANAGEMENT?

The most frustrating part of being a risk manager is responding to people's misconception of what risk management is.

By Joan T. Schaming

Most people equate risk management with insurance. If you think about it, that is quite absurd. Is buying insurance the only way to manage risk? Of course not.

Insurance is one aspect of risk management, but certainly not the only one.

Then there are the operations managers who equate risk management with disaster recovery.

This too is only one aspect of managing risk. What concerns me most with this thought process is that these managers are only concentrating on reaction, recovery and restoration. ***There seems to be no thought given to proactive planning and prevention.***

Even though insurance and disaster recovery are necessary parts of risk management, both will hopefully never be needed. That's where end-to-end risk management comes into play.

So, what is this thing called risk management?

Let's take a look at the definition of risk management. The dictionary defines risk as "possibility of loss or injury" and management as "the art of handling or directing with a degree of skill; to treat with care."

The definition of risk management, therefore, should quite simply be: "the art or act of handling the possibility of loss or injury." Furthermore, this shows that risk should also be treated with care and taken seriously.

Let's now look at the four components of risk management: Indexing, Assessing, Mitigating and Measuring.

INDEXING

The first component of risk management is knowing what needs to be managed. **Indexing is an easy way to determine what are the critical operations of the company or organization.**

It is important to remember that not every operation or business function is critical and, therefore, the loss of non-critical operations for an expanded period of time will not cause financial hardship to the company or close down the business.

For example, payroll is a vital business function as employees must receive their scheduled pay checks. Training, on the other hand, can be suspended for several months with little or no effect on the company's financial state.

Once the critical operations and business functions are determined, a profile should be developed linking supporting factors to them.

This should include suppliers, system and applications, list of users, security, contractual commitments and regulatory requirements.

At this point, a rating should be assigned to each operation or business function denoting its criticality level to the company or organization. The criticality rating is then used to prioritize all of the operations and business functions to determine which needs to be assessed further for risk exposure and mitigation.

Often, time is spent on developing a sophisticated, mathematical model to achieve this. If you have the time and resources…great! But a simple *vital/important/deferrable or high/medium/low* will accomplish the same purpose. The important thing is to document the rating definitions so that they are applied equally to each operation or business function.

ASSESSING

Once the operations and business functions are indexed and a priority list determined, **the next step is to conduct an assessment of risk exposure for those designated as 'vital' or 'high.'** A risk assessment should be done on all critical operations and their associated business functions. There are several approaches to risk assessment. The one that has been valuable in my work is the **Loss Scenario Approach.**

This requires a risk management facilitator or expert to lead a team of subject matter experts in the **identification of risk, the rating and ranking of these risks** and the development of corrective and preventive actions.

The loss scenario method joins risk assessment and process management together.

The first step is to document the operational process. A profile should be developed which includes a definition of the process, step-by-step process flow, suppliers, inputs, outputs, customers, work centers supporting the process and monthly or annual revenue generated by the process.

Once the process definition and flow are complete the risk assessment team will analyze each step in the process flow to determine "What can happen?". The product of this step is a list of risks.

From that list, risk or loss scenarios are developed, creating a short story of the factors that could contribute to the risk occurring and then bringing that to the worst case. Preventive and/or corrective actions are then identified focusing on the contributing factors.

This is only one approach for assessing risk. There are many others that you may be familiar with such as Root Cause or Fault Tree Analysis. However, I have found the loss scenario approach the best for assessing risks in a process. Both root cause and fault tree analysis work well for more technical reviews. Whether the loss scenario, root cause or fault tree approach is used, preventive and/or corrective actions are then defined for each cause and recommendations are developed.

MITIGATING

The mitigation phase of risk management is where the lead role changes from the risk manager to the specific operations manager or business function owner.

It is here that the recommendations from the risk assessment are reviewed and management decides which risks need to be addressed and which can be accepted. ***A risk mitigation plan is then developed outlining who, what, when and how the corrective and preventive actions will be implemented.***

You will soon discover just how seriously management wants to manage risk, for **mitigation does cost money and requires resources.**

At this point a cost benefit analysis may be needed to show management that the output of mitigation cost far outweighs the loss of revenue, loss of life or cost of recovery.

For example, all three preventive actions shown in the "Sample Loss Scenario" (see below) are relatively inexpensive to implement and certainly outweigh the loss of human life.

Regardless of the type of business or size of your company, the risk mitigation plan must always include insurance and disaster recovery planning.

It should be noted that your company or organization ***could actually save on insurance if they have an active risk management process in place.***

MEASURING

Plans can be written, applications can be backed-up, data can be stored or replicated and insurance policies can be bought, but that does not necessarily mean that your company or corporation is free of risks or even that the mitigation efforts are effective.

The last component of risk management, therefore, is the testing and measurement of the effectiveness of the corrective and preventive actions.

Testing disaster recovery plans, testing alarms and procedures, conducting building inspections and reviewing building incident reports are some sources of effectiveness measurements. Whichever measurements are chosen, it is important that management be honest in the results. It serves no purpose to cover up poor results, for they are the warning signs that the corrective actions are not working.

In the fire scenarios for instance, (see below) the second preventive action calls for periodic inspection of all electric appliances in the facility. What if management decides to do this inspection only once a year?

A review of the building incident reports could disclose that two other appliances caused minor fires in the last three months. Thus an annual review would do little to mitigate this risk and this preventive action would prove to be less effective than originally intended.

In closing let's take another look at the definition of risk management which we spoke about earlier; "the art of handling or directing the possibility of loss or injury".

Yes, risk management is an art and like any work of art it is valuable, something to be admired and worth its weight in gold.

About the Author:

Joan T. Schaming, CDRP, is Risk Manager for AT&T Continuity Services, Warren, NJ. For more information, call (908) 580-6944 or email jschaming@att.com *Reprinted with permission of Survive! Magazine, February 1997. For more information about membership in Survive! the international association of business continuity planners, phone 800 SURVIVE or email* surviveusa@aol.com *Also, visit the web site at* www.survive.com

---

LOSS SCENARIO

Risk: FIRE

A faulty wire on the microwave in the employee lounge causing a fire which spreads rapidly throughout the floor. Two employees in the immediate vicinity of the microwave are seriously injured while trying to put out the fire with water. Another employee attempts to rescue the injured but is overcome by carbon monoxide fumes. His absence is not noted until the fire has been contained by the fire department. All three employees are later found dead.

PREVENTIVE/CORRECTIVE ACTIONS

1. Ensure the existence of adequate fire extinguishers and alarms. If inadequate, acquire necessary equipment.
2. Conduct periodic inspections of all electrical appliances in the facility for defective cords, connections, etc. Where necessary, replace appliances.
3. Develop a fire evacuation safety plan which includes the assignment of fire marshals who are responsible for a group of people in the event of a fire. The plan should also include the training and testing of the evacuation procedures. The procedures should be reviewed with all employees at least semi-annually.