Risk

This section is also known as a simple approach to risk. I emphasize this simple approach as it is often easy to slip into a complex web of risk assessments that can muddy the waters and prevent the team from having a clear focus on the real issues.

There are a myriad of theories and writings and approaches to risk. Risk Identification, Risk Analysis and Risk Management will all produce thousands of valued resources and sources of advice when searching on the internet.

With all of these sources of information comes confusion and it can be difficult sometimes to sort out the practical usable material from the theoretical science.

Risk is simply defined as the potential for an event to occur. Risk assessments should focus on what is real and not purely theoretical. When dealing with projects, systems, servers and networks there are a fixed set of risks that should be considered for most applications. Then when the use of the system is considered within the business environment, the risk list can grow. When we begin to look at the impact of the risks either direct or indirect, the results can vary.

Consider a very simple example. There is a risk that anyone of us could be struck by lightning. The likelihood of occurrence is low, the impact is quite high (life threatening) and the likelihood of detection is high (as you or those around you will know fairly instantly). The overall risk is therefore low. In other words, we don’t have to concern ourselves or protect ourselves from a lightning strike every day.

Consider another example. There is a risk that anyone could catch a cold on any particular day. The likelihood is moderate as you only need to come in contact with the virus to catch the cold. The impact is low because the symptoms although inconvenient will only last a few days and the likelihood of detection is high. Therefore the overall risk is rating is low.

Convinced yet?

We will look at a couple more examples as we move through the chapter.

The process of risk in a project or series of tasks usually looks like this:

- Identify the Risks
- Analyse the Risks
- Manage the Risks

A risk identification meeting whether it is relating to a project, an operation or an investigation normally starts with a brain-storm of potential risks. This is meant to be an interaction where people that have experience and knowledge in the specific topic are asked to identify potential risks associated with a system, a project, an activity or a problem. It may take more than one session to identify the risks. As you proceed through a project or an investigation risks can change, be eliminated, added and re-assessed.

This session or these sessions need to be controlled. You should manage your audience here. So called "Experts" should be validated in their field before contributing. A useful tip here is to abide by the golden rule of Risk Identification Assessments – "If you raise a Risk -You Own that Risk" . You will need to perform all the little tasks associated with that risk but you at least have a responsibility for reporting. Manage any mitigation actions associated with the risk until it has been closed or is no longer relevant to the body of work.

Following this rule serves distinct purposes:

- It makes everybody think very carefully about adding risks casually without any thought going into them – i.e. – is this a real risk or not?
- If someone does raise a risk, then they should already be thinking about a management strategy for that risk and therefor provide a better quality of "risk" to the risk identification assessment.

The reason why caution is advised here is that in many organizations once a risk is raised it has to be managed through a process, it cannot simply be removed. This process needs to be formally agreed and in some cases approvals sought before the risk can be removed. From my own experience, at the beginning of a large project or investigation there tends to be a lot of "Talkers" present and they will feel the need to say something rather than just staying quiet if there is nothing to say. Loose words spoken at the start of a project can cause a lot of "non value ", resulting in managing a risk that is either so far-fetched it is impossible, or that it is just not relevant for this body of work.

So just so we do not labour the point too much here – ensure you have the right people in the room and they are aware of the golden rule.

Once it has been agreed and the risks have been identified – it is then necessary to analyse or review the risks to assess their risk rating. This topic will also spurn much conversation and debate about the best way to do this. Below is a summary of an advised approach, although most organizations will have their own specific risk assessment process, this following method certainly covers the bulk of them and makes the process very clear.

- What is the likelihood of occurrence of the issue? Rate from 1 – 10.
- 1 = Least Likely – 10 Most Likely.
- What is the actual Risk – Provide a description here. What is the actual issue that will occur if the risk comes to pass?

- What is the impact of that risk – 1 to 10. 1 = Low Impact- 10 = High Impact

The next item is the most overlooked element of risk in industry today.

- What is the likelihood of detection of the problem? Rate from 1 to 10.
- High Likelihood of Detection 1 — 10 – Low Likelihood of Detection

The paradox here with "likelihood of detection" is that if an issue is easy to detect, the overall rating of the risk is reduced. If the issue is difficult to detect, the overall rating of the risk is increased.

The risk number or risk rating is calculated as follows:

Likelihood of Occurrence X Impact of the Risk X Likelihood of Detection

If we look at the numerical possibilities here – Lowest Risk Case Number is 1 Highest Risk Number is 1000.

i.e. 1 x 1 x 1 = 1

10 x 10 x 10 = 1000.

Let's look a couple of simple examples to help explain this:

Risk Topic	**Number**	**Total Number**	**Rating**	**Explanation**
Occurrence	5	5	Low Risk	Although the likelihood of occurrence is high the impact is low and the likelihood of detection is high. Therefore, the overall risk is low
Impact	1			
Detection	1			

Risk Topic	**Number**	**Total Number**	**Rating**	**Explanation**
Occurrence	2	24	Low	Although the likelihood of occurrence is low the impact is moderate and the likelihood of detection is low. Therefore, the overall risk is medium.
Impact	3			
Detection	4			

Risk Topic	**Number**	**Total Number**	**Rating**	**Explanation**
Occurrence	8	506	Medium to High	Although the likelihood of occurrence is low the
Impact	7			
Detection	9			

Risk Topic	Number	Total Number	Rating	Explanation
				impact is moderate and the likelihood of detection is low. Therefore, the overall risk is medium.

Risk Topic	Number	Total Number	Rating	Explanation
Occurrence	10	900	High	Although the likelihood of occurrence is low the impact is moderate and the likelihood of detection is low. Therefore, the overall risk is medium.
Impact	9			
Detection	10			

As mentioned earlier, when looking at individual risks – you need to have the right people in the room. These must be the SMEs (Subject Matter Experts) that have experience in a particular field and can answer any queries with little effort and time spent.

The objectives if analysing risks and managing risks are to:

- Clearly understand the risk. You need to understand the risks in order to manage them. Often someone's lack of understanding of a problem can lead to a risk being added to the risk list. In any industry you need to keep up with technological advances and ensure that your software, servers networks and systems are getting the benefit of new technology. If a system is risk assessed and 2 years later a follow up risk assessment is performed, the delta in the results can be startling. Mobile technology, remote control, wi-fi, networks, backup and recovery capability have all had huge improvements in functionality and benefit in recent years.
- Eliminate the Risk – Most preferential Solution – a very simple example. A server is old and uses a non-supported operating system. The hardware is performing badly and un reliable. To eliminate the risk in this case you would replace the sever with a new model and up to date operating system.

Initial Risk Rating will be high.

- Mitigate the Risk – to reduce the impact if the risk by specific measure - Old Server – Perform a clean up of the server, increase memory space, up[grade the processor, install latest patches perform a virus check and ensure the server is operating as expected. These actions will reduce the risk of failure of the server occurring.

Mitigated Risk Rating will be lower than the original

- Manage the Risk – Perform regular maintenance and performance monitoring of the Server to ensure that memory capacity does not exceed recommended limits. Anti-virus is up to date and CPU processing capacity is adequate and does not doses not display any high usage.

The ongoing risk rating can be reduced once the mitigation measures are proving effective.

(In rare circumstances, it may only be possible to accept the risk, acknowledge the risk and proceed with caution. You may need to have a contingency plan to put in place should the potential event come to pass as identified in the Risk Assessment. Be careful here to document the decision to accept the risk with the main stake holders in the situation. Accepting the risk and having a back up plan is quite different from doing nothing. Doing nothing is a conscious decision not to do anything – it is not a passive by standing status that allows you to wash your hands of all culpability should the worst case come to pass.)

In this simple example, we can illustrate how the risk is addressed. Let's consider the case of an outdated server that is unsupported by any vendor, has an old unsupported operating system installed and is experiencing performance issues due to low processing capacity and storage issues.

To follow up on this one and provide more detail, the ideal scenario is to replace the server. It may not be possible for the server to be replaced at this time. What on the surface may seem like a simple task may have far reaching implications particularly if:

- The server is running a business critical software application.
- There may be a substantial effort and financial commitment involved in upgrading the application on to the new server.
- The new server may have a different physical foot print in the IT Server Room.
- New Power Supplies may be required.
- Other servers may be impacted.
- This work may only be possible during a power outage or during a shutdown.

The risk mitigation measures will have an overhead as there may be a requirement to monitor the vital operating parameters weekly or daily. The effort here should be considered. If these parameters are monitored by software - the software may create an overhead on the server. Which in itself may need to be risk assessed.

As a general guideline in most industries, no high risks should be tolerated without a short term definitive plan for tackling that risk in order to eliminate the risk or to severely reduce the three influencing factors, likelihood of occurrence, severity of impact, and likelihood of detection.

There is a huge temptation in a fast moving operational environment to implement a quick temporary fix in order to be seen to mitigate the risk. Be careful here as I know of many temporary fixes in business all over the world that remained in place for 10 years or more.

As this book is largely concerned with the troubleshooting of issues and the implementation of remedial actions, we need to focus on the risks of our actions. i.e. what are the risks associated with the course of action that we intend to take to resolve the current problems?

This requires as much thought an attention as the investigation to find the root cause.

Let's illustrate this with another example

A network switch is operating intermittently and resulting in communication errors across a network. The errors are resulting in a series of problems for business applications and flooding the IT Help Desk with calls consistently over a period of one week. The team has eventually isolated the issue to the network switch. The manufacturer if the network switch has indicated that the Firmware (Operating Software) on the switch needs to be upgraded. The vendor offers to do this remotely and maintains that this can be done in less than 20 mins with minimal disruption to operations.

The IT Engineer allows the vendor to log on to the switch remotely – download the firmware and perform he install. During the upgrade the switch freezes and will not reboot. All communication across the switch is lost for a number of hours - major disruption to the business applications dependent on the switch. A new switch is then ordered and takes a day to arrive. Meanwhile network traffic is re-routed connecting to another switch. That switch becomes overwhelmed and communication is affected across that switch due to the additional traffic and this then affects another area of the business previously unaffected by the first issue. The original troubled switch is replaced and the network connections are re-established and normal operational performance is resumed. The IT Director and his/her team are red faced and have to explain what happened and why, how the issue was resolved and what measures are in place or what actions are planned to prevent a recurrence.

Does this should familiar?

Let's take a look at what happened, why it happened, what was done, what should have been done and what needs to be done to prevent a recurrence.

What happened was that a problem was observed and isolated to the switch firmware as the root cause. With no risk assessment of the proposed course of action, the firmware was updated. This caused further issues and longer to recover. There was no spare or equivalent switch on site that could have been utilised.

What should have happened was that a risk assessment of the actions to be taken should have been performed. The Risk Assessment would have identified the risks associated with the Firmware upgrade.

The results of the risk assessment would have called for mitigation in the form of a back-up plan- i.e. to source an replacement switch and have it pre-programmed ready to go. This would have reduced any downtime associated with the switch failure.

After the fact reviews of what went wrong can be a great source of learning and when reviewing the actions with the comfort of time and space, the poor decision made under pressure can seem almost ridiculous.

Affording the right people time to think about the problem can save you time and money in the long run. Knee jerk reactions should be avoided if possible. Company culture can have a huge influence on how problems are assessed and investigated. Culture within an organization cannot be changed overnight. It will take a considerable effort and a lot of time to turn a culture around. By becoming disciplined in your approach to troubleshooting and following a proven process, results will be obvious. As you begin to deliver results, trust will soon follow. It doesn't take a long time in a large company to acquire a good (or bad) reputation. A couple of high level investigations managed well and to a successful conclusion will go a long way to securing that reputation.