Understanding and Responding to I.T Risk

An Overview

Ismail M. Settenda

ICT-Pros Consultants Ltd

Managing Risks Checklist

- Introduction (what, who why and when.?)
- Planning for Risk Management..?
- Risk Management Methods
- Risk Management Strategies and Procedures
- Risk identification and measurement tools
- Sample Risk Management process flow

Overview

Before we start lets make some recollections and reflections on

- What is risk and how does it factor in I.T projects.
- What is an I.T project.?
- What is risk planning and management (*failing to plan means you..?)*
- What are the main sources of risk?
- Lastly what is Risk Management/Mitigation.

Discuss

Assume you have been assigned an assignment to initiate, develop and implement a secure mail server or similar I.T project.

- How will you ensure its success?
- How will you limit failures and resolve vulnerabilities?

Before we start can I.T project

There are a few simple things to think through and do at the start of any project:

Who is going to be affected (directly and indirectly) or involved, including supporters and detractors? What will be their influence?

Are there steps we should add to the activity to ensure success? For example, a test run or have an expert review the plan.

Do we have a plan in place to manage scope and change effectively?

What is I.T Risk Management.?

Risk Management can also be viewed as a methodology that helps I.T project managers make best use of their available resources.

We should know that Risk Management is one of the knowledge areas or elements of project management and that it focuses on improving the chances of successfully concluding a project, so we can also say that it is;

- Good management practice
- Involves process steps that enable improvement in decision making
- A logical and systematic approach to
  - Identifying opportunities
  - Avoiding or minimizing losses

I.T Risk management is therefore the process concerned with identifying, analyzing and responding to risk in any I.T endeavor or project.

When do we do Project Risk Management?

I.T projects we know that **'Risk'** is *dynamic and subject to constant change(one keystroke can change a lot in a very very short time).*

To achieve success good planning is necessary as well as being able to early on understand the risk and uncertainties associated with the project.

Discuss at what stage one will know these risks?

- When the *Sh**%$#t…hits the fan..?
- Refer to project cycle stages and make reflection at which stage is critical (*idea/problem-plan-execute-monitor-close*)
- Is it during appraisal stage, where and when?
- When the projects resources are constrained?
- When business management derives greatest value ?
- Analyzing schedule and cost risks?
- Quality of the final products or what?

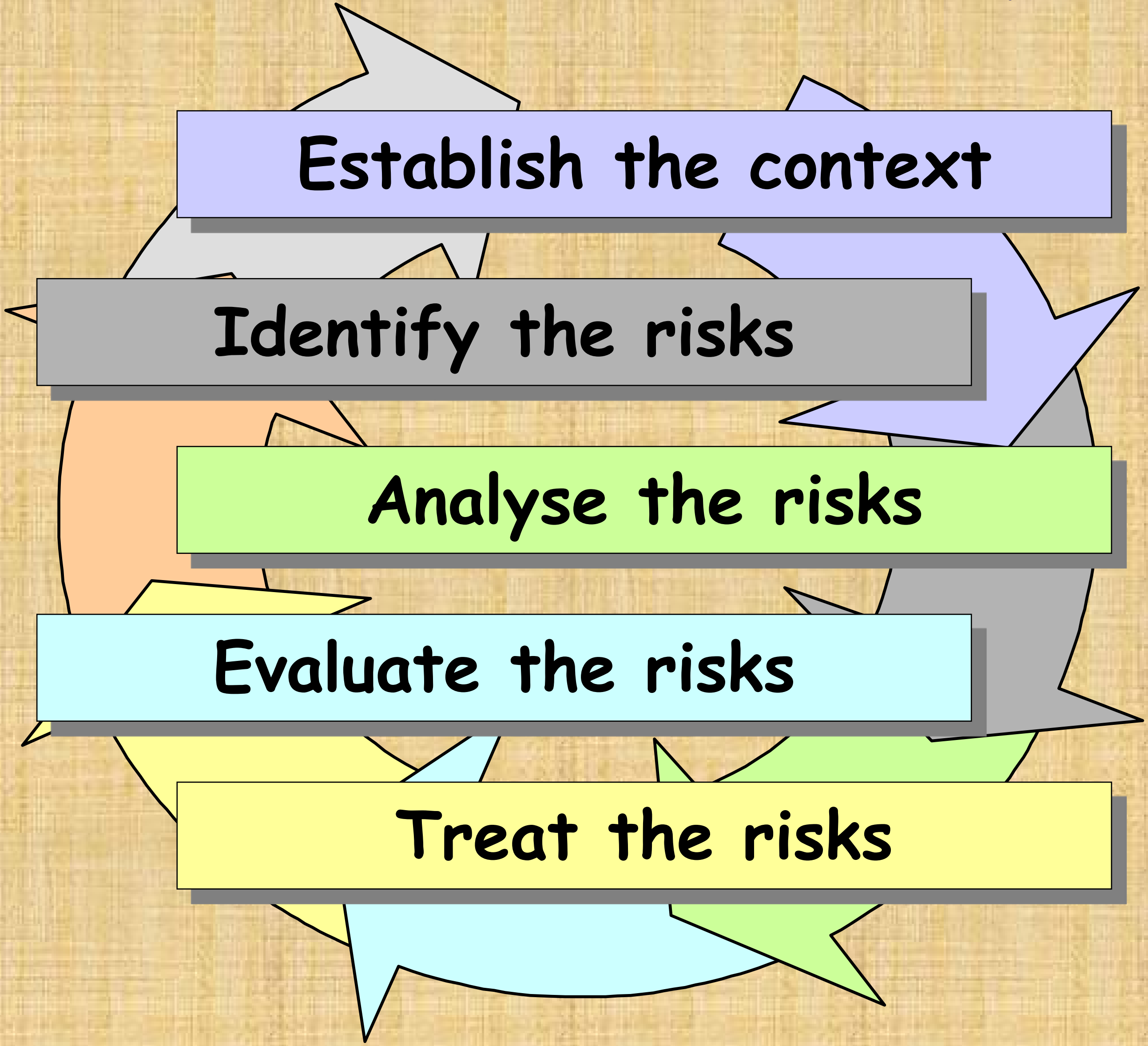
So it seems the process will have to include continuous **Monitoring** and **Review** as well as **Communication** and **Consultation**. (M&R with C&C).

I.T Project Risk Management Overview

- Make a plan for the dealing with risk
- Identify Risks
- Qualitatively analyze these risks
- Quantitatively analyze these risks
- Plan a Risk Response
- Communicate
- Monitor & Control

The Risk Management process

We will combine them to get these basic process steps:



Establish the context

Identify the risks

Analyse the risks

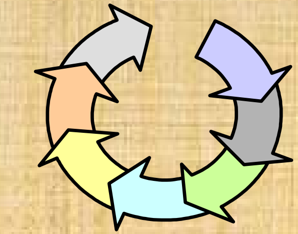
Evaluate the risks

Treat the risks

Here we see that !

- **Identify Risks** is the process of determining which risks may affect the project and documenting their characteristics.
- **Perform Qualitative Risk Analysis** is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.
- **Perform Quantitative Risk Analysis** is the process of numerically analyzing the effect of identified risks on overall project objectives.
- **Plan Risk Responses** is the process of developing options and actions to enhance opportunities and to reduce threats to project objectives.
- **Monitor and Control Risks** is the process of implementing risk response plans, tracking identified risks, monitoring residual risks, identifying new risks, and evaluating risk process effectiveness throughout the project.

The Risk Management process



Establish the context

The strategic and organisational context in which risk management will take place.

For example, the nature of your business, the risks inherent in your business and your priorities.

Communicate & consult

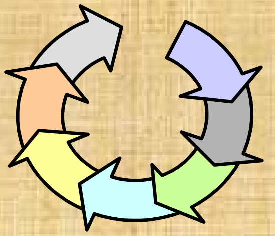
When thinking of I.T project risks and uncertainty analysis, what are we referring to ?

In what context can risk be viewed as;

- **Getting hacked?**
- **Losing data/information?**
- **Corruption/contamination of the data/information?**
- **Cost of added IT hardware and software, and/or a composite of resource investments such as skilled labor and associated salaries?**
- **The opportunity cost of deferring other tasks or works.**

Assuming you going to do something about the risk then >>…?

The next step in the RM process



Risk identification

- This typically comes when much of the initial plan is done
  - It answers the "hows" of our plan can be used to determine the sources of risk we need to look at.
- Get the team together to review the sources of risk for our project, brainstorm the specific risks, then have some of the local subject matter experts review the generated list.

How can you identify Project Risks

- You will undertake an initial risk assessment as part of starting up the project. Basically you will ask these questions:
  - What could possibly happen to affect the project?
  - What is the likelihood of this happening?
  - How will it affect the project?
  - What can we do about it?

- It is helpful to consider that the source of the risk is called the risk cause (the potential trigger points for each risk),
- The risk event describes the area of uncertainty, and the risk effect which describes the risk impact on the project objectives.

How can you identify Project Risks…contd

- Brainstorm the risk possibilities to determine main internal and external risk sources.
- Consult experts and those who monitor external conditions to determine risk
  - what's the likelihood of rain or an earthquake during our construction project?
  - will a new operating system or software derail our software project?).
  - What about language compatibilities..?
- Examine risk sensibly
  - a process commensurate with the levels and impacts of risk) and
  - statistically (Did you know air travel is safer than travel by car?).

Risk Identity Techniques

1. Documentation Reviews
2. Information gathering Techniques
   1. Brainstorming
   2. Delphi Technique
   3. Interviewing
   4. Root cause analysis
3. Checklist Analysis
4. Assumptions Analysis
5. Diagramming Techniques
   - Cause and effect diagrams, system or process flow charts, Influence diagrams etc.
6. SWOT Analysis
7. Expert Judgment

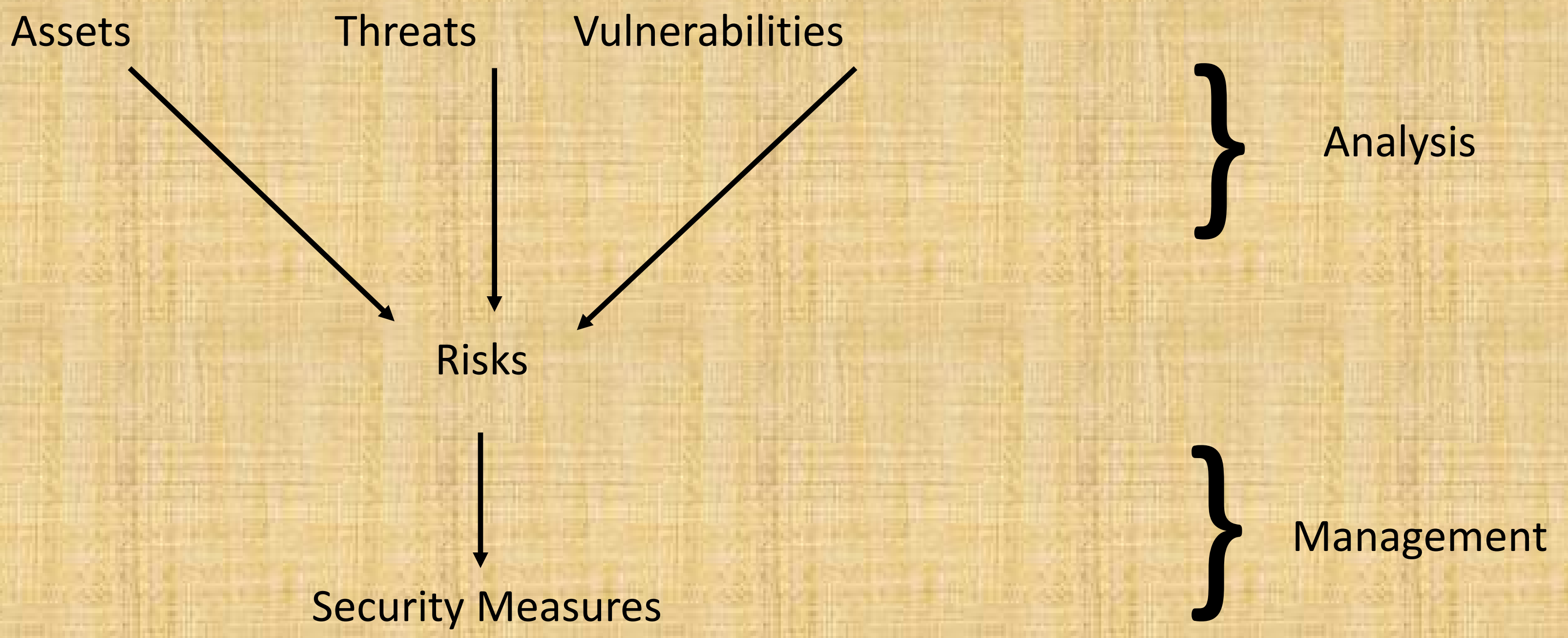
TYPICAL RISKS SOURCES

Our I.T projects face many sources of risk. Here are just a few:

- Legal (patents and lawsuits)
- Corporate policy and procedural changes
- Changes in technology
- Natural hazards and conditions (have you seen the latest volcano /hurricane/Political news?)
- Client driven scope changes
- Out of balance cost, schedule, or quality..?
- Unplanned for events and change
- ..?
- ..?
- ..?

Doing the Risk Assessment/Analysis

Risk Analysis and Management Framework



Assets

Threats

Vulnerabilities

Risks

Security Measures

Analysis

Management

The Goal of Risk Analysis

- All assets have to be identified
- All threats have to be identified
  - Their impact on assets has to be valued
- All vulnerabilities have to be identified and assessed

SWOT Analysis

This technique examines the project from each of the SWOT (Strengths, Weaknesses, Opportunities, and Threats) perspectives to increase the breadth of identified risks by including internally generated risks. The technique starts with identification of strengths and weaknesses of the organization, focusing on either the project organization or the wider business.

These factors are often identified using brainstorming. SWOT analysis then identifies any opportunities for the project that arise from organizational strengths, and any threats arising from organizational weaknesses. SWOT analysis also examines the degree to which organizational strengths offset threats and opportunities that may serve to overcome weaknesses.

Step a:Risk Identification (Threats)

Identification and valuation of threats - for each group of assets

- Identify threats, e.g. for stored data
  - Loss of **confidentiality**
  - Loss of **integrity**
  - Loss of **completeness**
  - Loss of **availability** (Denial of Service)
- For many asset types the only threat is loss of availability
- Assess impact of threat
  - Assess in levels, e.g H-M-L or 1 - 10
  - This gives the valuation of the asset in the face of the threat

Step b:Risk Identification (Process)

- Every company or organisation has some processes that are critical to its operation
- The criticality of a process may increase the impact valuation of one or more assets identified

So

- Identify critical processes
- Review assets needed for critical processes
- Revise impact valuation of these assets

Step c:Risk Identification (Vulnerabilities)

Identify vulnerabilities against a baseline system

- Risk analysis of an existing system
  - Existing system with its known security measures and weaknesses (Win XP)
- For development of a new system
  - Security facilities of the envisaged software, e.g. Windows 7 or Linux
  - Standard good practice, e.g. BS 7799 recommendations of good practice

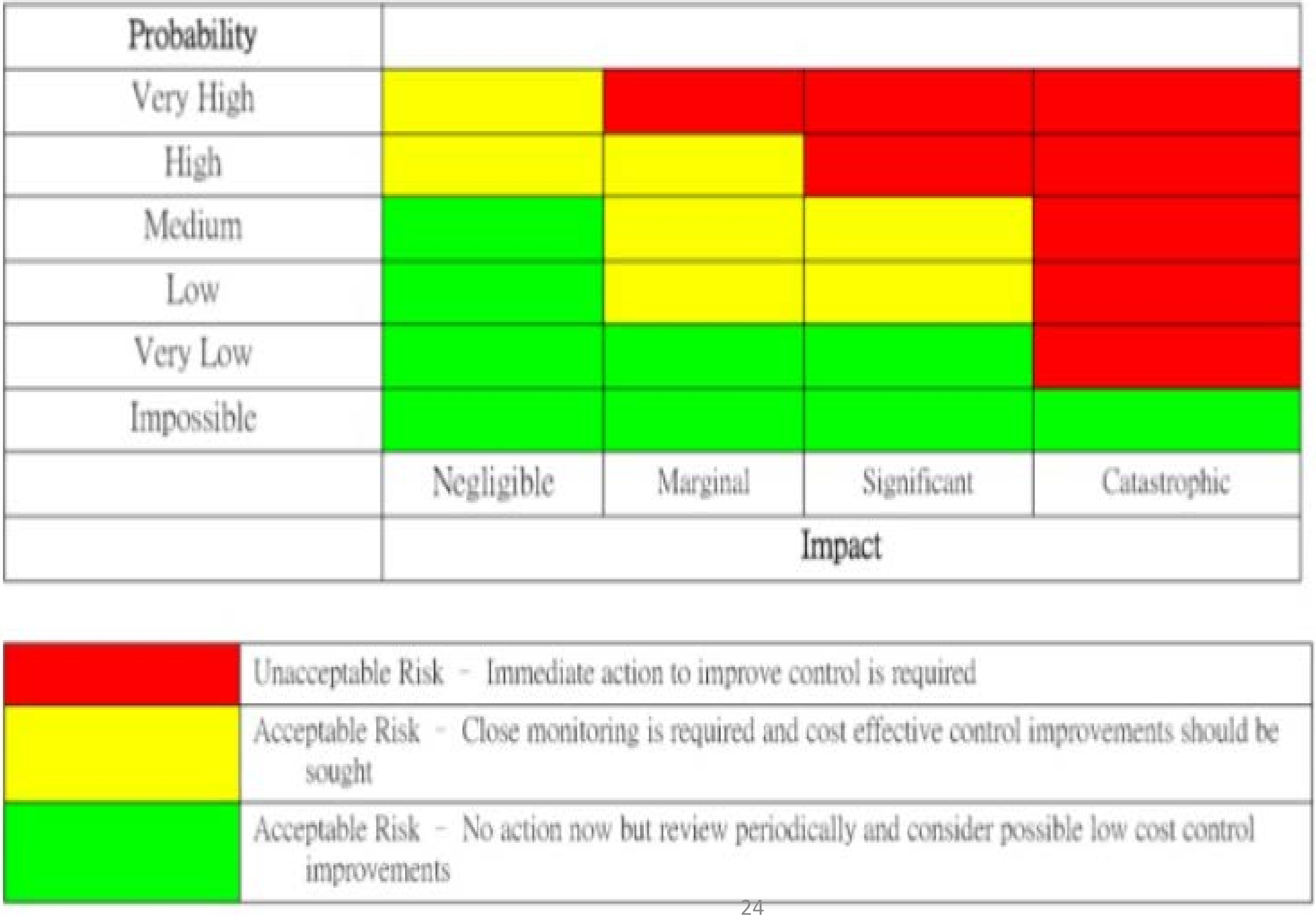
For each threat

- Identify vulnerabilities
  - How to exploit a threat successfully;
- Assess levels of likelihood - High, Medium, Low
  - Of attempt
    - Expensive attacks are less likely (e.g. brute-force attacks on encryption keys)
  - Successful exploitation of vulnerability;

The Levels of Risk

- Precise monetary values give a false precision
- Better to use levels, e.g.
  - High, Medium, Low
    - High: major impact on the organisation
    - Medium: noticeable impact (“material” in auditing terms)
    - Low: can be absorbed without difficulty
  - 1 - 10
- Express money values in levels, e.g.
  - For a large University Department a possibility is
    - High
    - Medium
    - Low

- PI matrix



Probability				
Very High	🟨	🟥	🟥	🟥
High	🟨	🟨	🟥	🟥
Medium	🟩	🟨	🟨	🟥
Low	🟩	🟨	🟨	🟥
Very Low	🟩	🟩	🟩	🟥
Impossible	🟩	🟩	🟩	🟩
	Negligible	Marginal	Significant	Catastrophic
	Impact			

🟥	Unacceptable Risk – Immediate action to improve control is required
🟨	Acceptable Risk – Close monitoring is required and cost effective control improvements should be sought
🟩	Acceptable Risk – No action now but review periodically and consider possible low cost control improvements

Continued…!

- Understanding ways of mitigating various risks, both known and unknown.
- Helps to understand risks prior to the project moving into the design and build, or development, or engineering, or whatever you call the phase where actual work takes place
- Analysis is one of the key pieces which, if not done with diligence could cause a failure of a project.
- Helps to ask relevant questions, but we also have to be sure that we follow-up to each question, and that we get answers

Responding to Risk

Here we are more subjective and qualitative in our analysis.

This is so we can plan our responses to risk (share, transfer, accept, avoid and reduce).

- **Share** collectively with other parties in dealing with it.
- **Transfer** it so it becomes someone else's problem/burden.
- **Avoid** it completely by withdrawing from an activity
- **Accept** it and do nothing
- **Reduce** it with security measures

N.B. As we plan our responses, we will need to alter our project plans.

And as we alter our project plans, we may introduce more risks, so we need to once again make sure we have identified all the risks.

Risk Mitigation Management Techniques

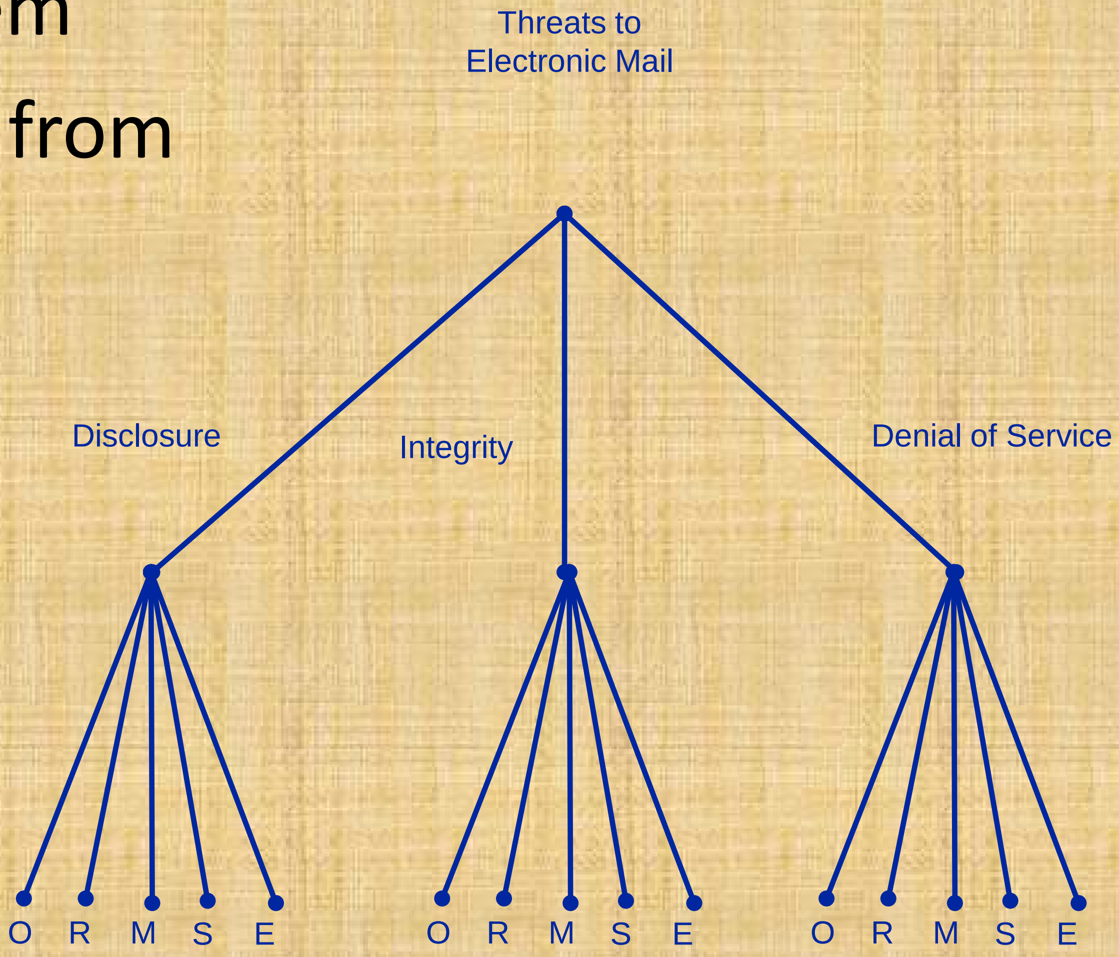
Commercial tools

- Mostly rely on check lists

- CRAMM (CCTA Risk Assessment and Management Methodology):
  - UK Government approach
  - Supported by software
- Risk Management softwares:
  - Gap analysis to identify necessary actions and existing strengths
  - Comprehensive practical guidance and the text of BS 7799
  - Reporting, for easy monitoring and maintenance
  - Evidence to customers and auditors

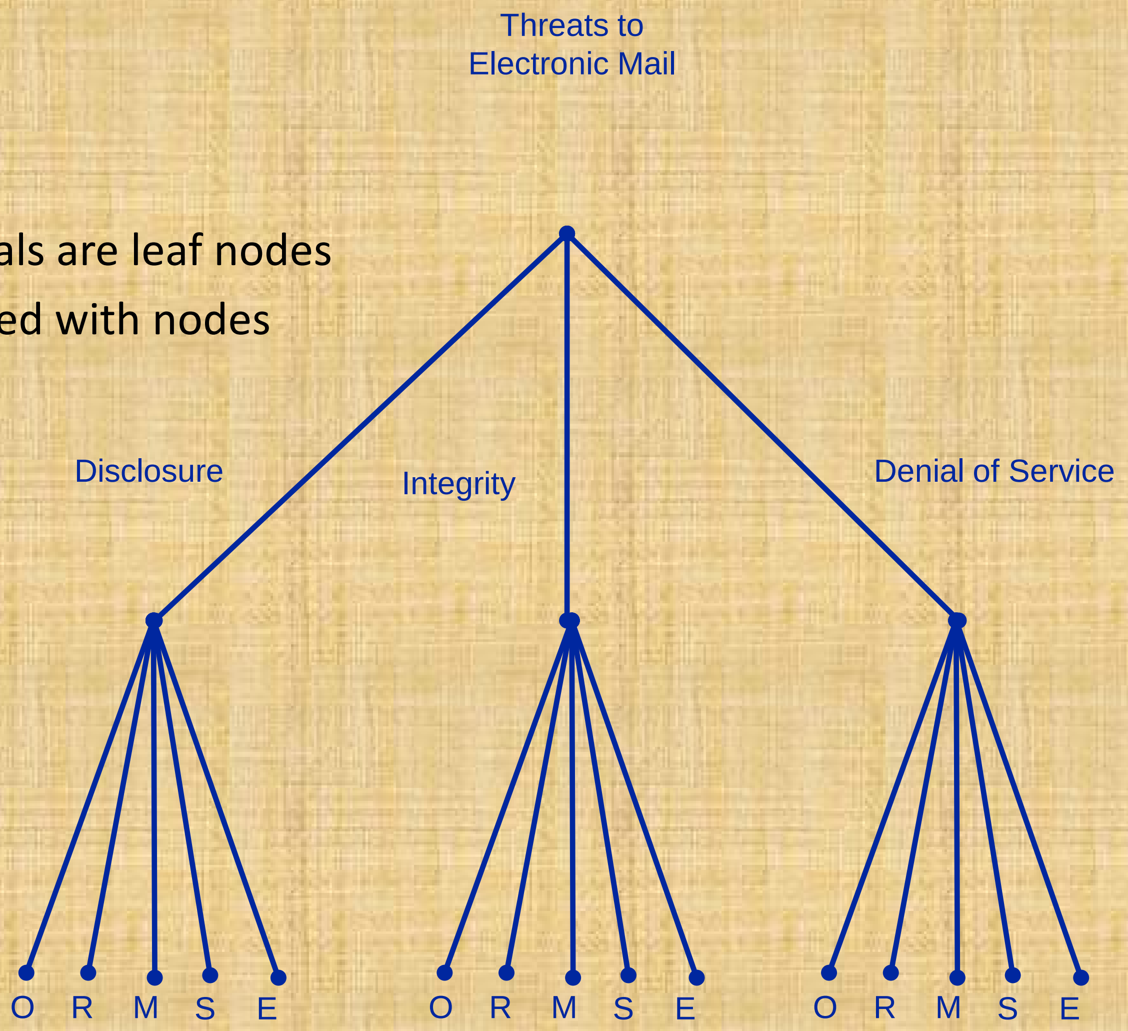
Threat Tree

- Model of system
- Calculate risks from
  - Impact
  - Vulnerability



Attack Tree

- Tree Structure
  - Goal is root node
  - Ways of achieving goals are leaf nodes
  - Costs can be associated with nodes



What Do We Need to know..?

- I.T Project Planning addresses issues of resource allocation e.g. money, time, people, capacity, etc.

- The I.T PP movement should be grounded in some financial objective such as not losing customers, increasing shareholder value, being the most secure, not being exposed or losing information..etc..

- Equally important, risks must be computed in a statistically or sociological meaningful sense.

- Optimizing resources and I.T projects with risks and uncertainties is most important throughout the organization and business development.

So is it sensible to use risk management in I.T projects?

- Risk management is a mechanism to help you to predict and deal with events that might prevent the I.T project outcomes being delivered on time.
- It clearly entails identifying each risk, and estimating it in terms of its probability and impact and controlling it by taking appropriate action and ensuring such actions have, and continue to have, the desired effect.
- This process should help I.T managers focus on priorities and in decisions on deploying limited resources to deal with the highest risks.
- Makes more effective use of existing skills and experience – giving better results.

General Statement

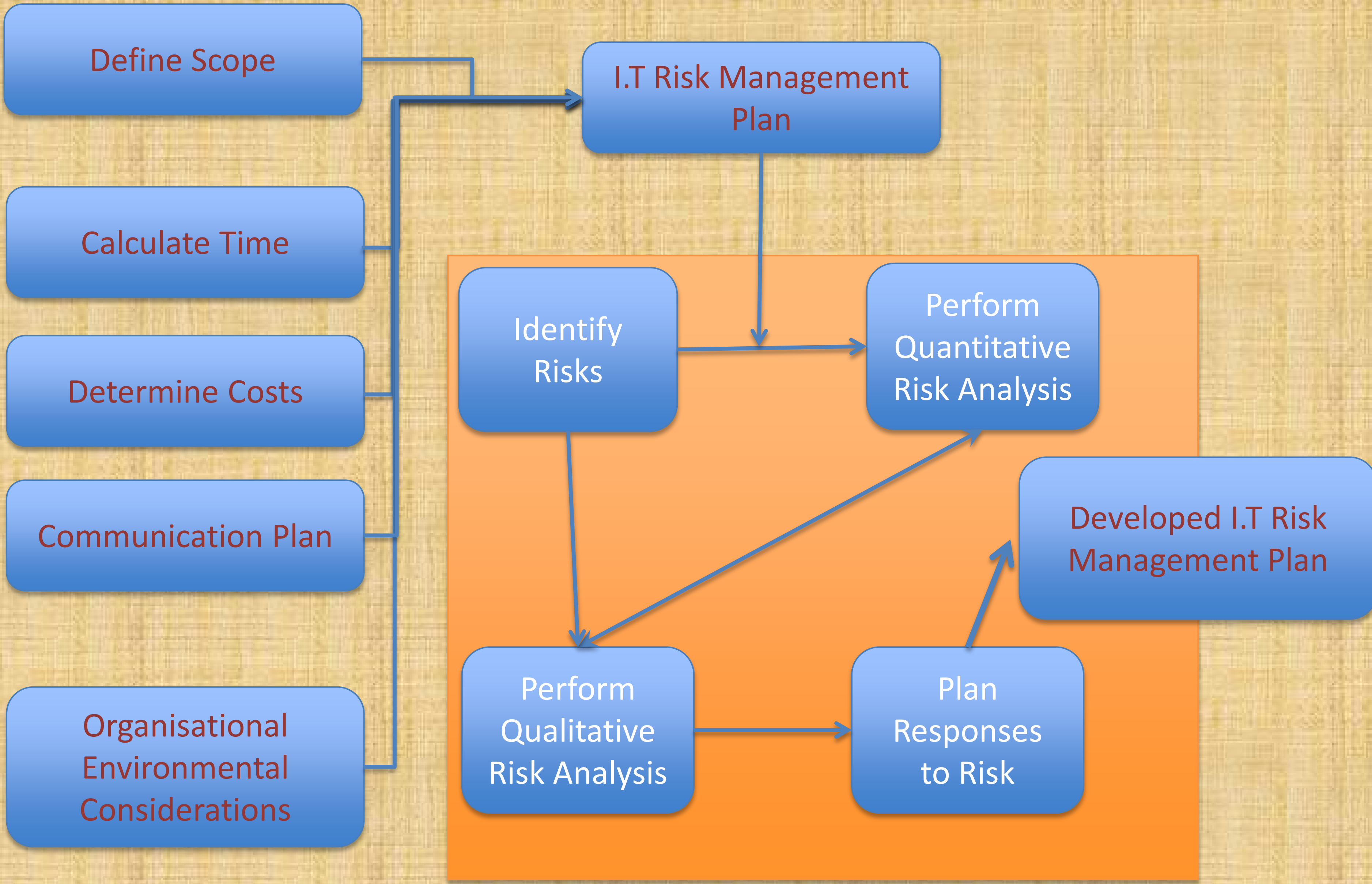
- Identifying risks is best done as a **team effort**.

- People with different skills, experiences and specialisms will see individual risks differently and you want a **balanced**, rather than a biased, analysis.

Discussion Checklist

- Scope (Environmental factors, organization policies)
- What will be the sources of risk.?
- What tools will you use to identification these risks?
- How will you determine what risk to deal with.?
- What risk management techniques and methods.?
- How will you set about mitigating these risks (strategy and procedure).?

Risk Planning Management Data Flow


Define Scope
Calculate Time
Determine Costs
Communication Plan
Organisational Environmental Considerations
I.T Risk Management Plan
Identify Risks
Perform Quantitative Risk Analysis
Developed I.T Risk Management Plan
Perform Qualitative Risk Analysis
Plan Responses to Risk

Adapted from PMBOK

Further steps

?

References

This presentation endeavored to briefly cover the concepts and the benefits of using Risk Management practices, particularly for IT. The processes and the many control options deserve further study, and many other sources of information on this topic are available from:

- **Project management book of Knowledge.**

- Visit: www.agenarisk.com (*download a FREE evaluation copy and build a risk map*)