Debate: risk management

Discussion leader: Pascal van Eck
University of Twente
Information Systems Group
p.vaneck@utwente.nl

Information Risk Management workshop
Enschede, May 31, 2007
Question 1

What do we expect from risk management (RM)?
• What should the results/outcomes of RM be?
• When are they good outcomes?
Question 2

Now that we know what ‘good results’ are:

What is needed to make risk management more efficient (equally good results for less effort/money)
Question 3

Now that we know what ‘good results’ are:

What is needed to make risk management more effective (better results, not necessarily for the same effort/money, could be more).
Question 4

Dynamic risk management (DRM): methods/tools that allow stakeholders to react to changes by taking informed decisions without having to carry out a full traditional RM cycle

Agree or disagree: current best practices in IT governance (such as CobiT) already ensure that the goals of DRM are met: they ensure that risks can be re-assessed and mitigated efficiently whenever there is a need to do so.
Question 5

Agree or disagree: RM as is currently carried out lacks the flexibility to keep the pace with organizational changes (both at the business and at the IT infrastructure level).
Question 6

RACI: Responsible, Accountable, Consulted, Informed

Agree or disagree: RM is a matter of determining RACI in the RM process. DRM is a matter of developing a tool that streamlines executing the RM process by supporting those who are Responsible or Accountable and by informing or consulting the relevant stakeholders. Any good workflow management system can be configured for that.
Information risk management research:

Should RM research be:

- **descriptive** (tell the work what *is currently being done*, conceptualize the current practice, harvest best practices)
- **normative** (tell the world how it *should be done*, invent new practices)?
Question 8

Case studies in risk management:

- Are case studies feasible?
- How about disclosure of results?
- What does it take to execute a case study?
Thanks!

Pascal van Eck
Department of Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands

p.vaneck@utwente.nl
http://www.cs.utwente.nl/~patveck