



IT Risk Management
Practice Guideline
online course

<http://www.cips.ca>

Stuff Happens ...



Bob Fabian, I.S.P.

instructor



- Former Chair, Computer Science, York University
- Former Partner,
💡 Gellman, Hayward & Associates
- Chair, CIPS Risk Management Task Force
- <http://www.fabian.ca>

CIPS on Risk Management


- “All professional assignments must begin with a risk assessment, and risk management must be practiced throughout professional assignments.”
💡
- May 2006

Session Objective

- Help the IT professional understand what it can and should mean to assess and manage IT risk.



Session Plan

- Motivation
- Definition of Risk
- CobiT Framework 
- Practice Guideline
- Responsibility
- References

It's a Turbulent World ...



Risk Motivation

- Social Concern
 - Turbulence is growing in society
 - Life become more unpredictable
 - Society requires those responsible to manage risk
 - Sarbanes-Oxley (or Bill 198)
 - Basel II for international finance
 - PCI for credit card processing



The Committee of Sponsoring Organizations of the Treadway Commission



- Enterprise Risk Management Framework (COSO - SOX Bible)
- *The challenge for management is to determine how much uncertainty the entity is prepared to accept as it strives to grow stakeholder value.”*

• July 2003

Risk Motivation II

- Professional Concern
 - Public expects professionals to be able and committed to manage risk
 - Professional needs the *intention* and the *ability* to manage risk
 - Intention: Code of Ethics
 - Action: Practice Guideline; Practice Recommendation; or Practice Requirement


Complications

- Professional no longer individual practitioner
 - More professionals practice in teams
 - Few independent IT professionals
 - Who has responsibility for risk?
- Shift from *know* to *assess*
 - Internet provides all the “facts”
 - Professional needed to assess

Trustworthy

- Deliver max-value/min-risk
- Except:
 - Value determined by client
 - Risk impact determined by client
 - And risk appetite/tolerance varies
- Appropriate value/risk balance

Risk Management

- *The* professional responsibility
 - Clients can recognize value
 - Expect professionals to identify risk
- Professional responsibility 
 - Before: Assess Risks
 - During: Manage Risks
 - Always: Communicate

IT Risk Complications

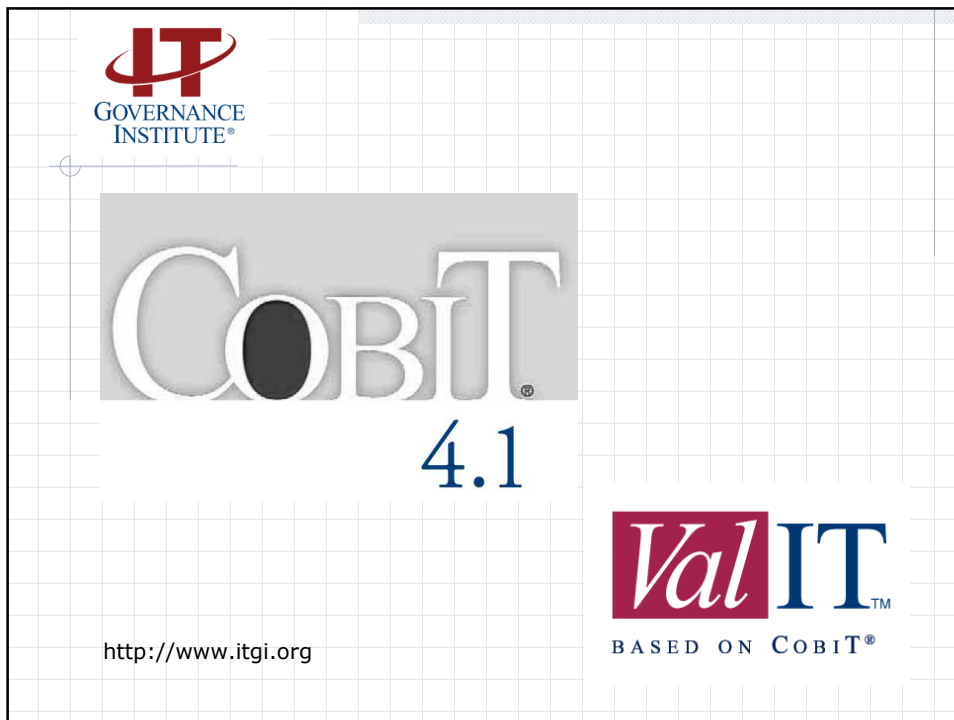
- Different kinds of IT risks
 - Acquisition, development, operations
- Different kinds of IT jobs
 - Programmer, manager, executive
- Different kinds of organizations
 - Risk appetite and tolerance
 - SOX, 198, HIPAA, Basel II, ...



- The IT Professional:
 - Must assess risk before assignment
 - Must manage risk during assignment
- Has Published
 - *IT Risk Management Practice Guideline*
- Will Publicize/Train
 - This is only the beginning ...

Risk Definition

- Risk is caused by an event which leads to an unplanned outcome
 - Can be positive or negative impact
 - IT often focused on negative impact
- Risk Severity = $P(\text{event}) \times G(\text{outcome})$
 - $P(x)$ = probability of event
 - $G(x)$ = gap between plan & actual



COBIT – IT Governance

- *The* IT Governance best practice
- Active harmonization efforts
- Maturity models for all processes
- RACI charts for all processes
- Risk relationships
 - Risk Management one of 5 pillars
 - Risk is one of 34 inter-related processes

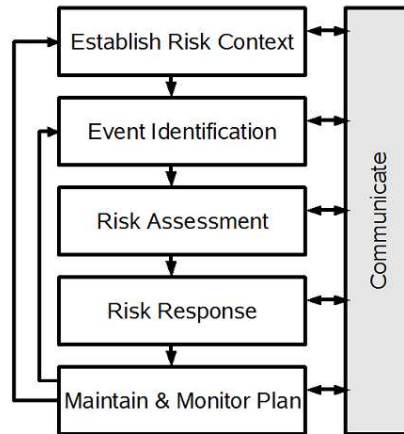
Practice Standards

- Practice Requirement
 - Full justification for all exceptions
- Practice Recommendation
 - Explanation for exceptions
- Practice Guideline
 - One of the approaches to consider

Practice Guideline

- Removes “ignorance” defense
 - I didn’t realize I should manage risk.
 - No one told me risk was my responsibility.
 - I didn’t know – I can’t be blamed!

CIPS Risk Management Flow



Tell Everyone ...



Communicate

- Important to tell people about risks
 - Above
 - Below
 - Besides
 - Following
- It's a *professional* responsibility
- It makes *business* sense

Risk Context

- What practices are to be followed?
- Event assessment
 - Who has a voice, how much detail?
- Outcome gap assessment
 - Who has a voice, how much detail?
- Risk response plan
 - Who has a voice, how much detail?

Event Identification

Four broad approaches

1. Judgement – individuals/groups use their best judgement
2. Scenarios – examine qualitatively different alternatives
3. Models – formally model the activities under review
4. Check Lists – use check lists or taxonomies of possible risks

Risk Assessment

- Assess *likelihood* and *impact* of all identified risk events
- Use quantitative *and* qualitative methods
- Determine *inherent* and *residual* risks
 - Effort to mitigate, then ...
 - How much risk remains?

Risk Response

Four broad approaches:

- Tolerate – live with the consequences, e.g. self insure
- Transfer – find insurance/contractor to assume the risk
- Reduce – change plans to reduce probability or impact
- Eliminate – don't engage in activities with unacceptably severity

Maintain & Monitor Plan

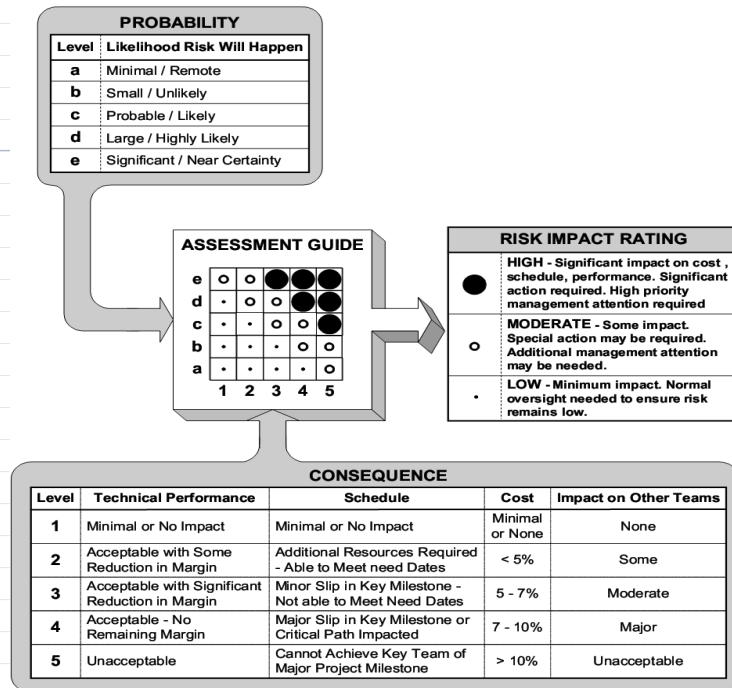
- Control activities to implement necessary risk responses
 - Costs, benefits, responsibilities
- Ensure committed actions are really owned
- Active monitor for risk events
- Monitor execution of plans
- Review/revise with stakeholders

Cost/Benefit is Important



From: US Air Force - GSAM version 3.0

US Air Force Approach



GSAM V 4.0

IT Activities

- Management (Strategy)
- Acquisition
 - Buy the wrong thing (bad spec/selection)
 - Thing evolves incorrectly (wrong dynamic)
- Development
 - Failure to meet the project's goals
 - Failure to address *real* opportunities
- Operations
 - Not adequately managing operations
 - Successful external attack on system

IT Professional's Approach

- Initial: Assess
 - Risk tolerance/appetite?
 - What can you identify?
 - How should you respond?
- Then: Manage
 - Plan response to risks
 - Monitor risk events
 - Execute on risk plans
- Always: Communicate

Remember

- Zero risk is a poor objective
- Find appropriate risk/value balance
- Val IT framework: Starting Point
 - It's the value balance to COBIT's control
- Always pay attention to value
 - It's the reason there is an IT

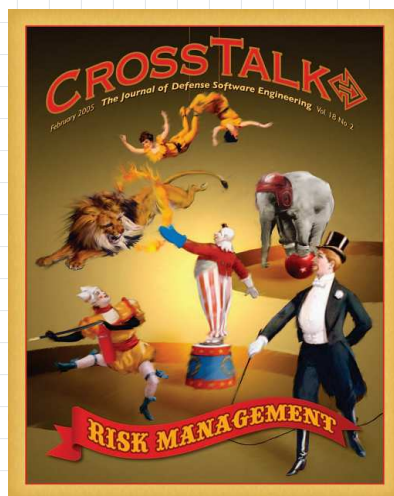
Selected References

Corporate Risk Management



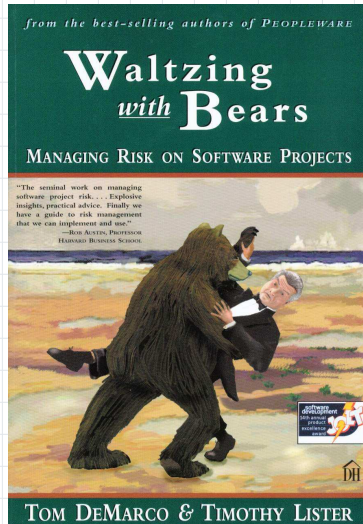
- Rotman Magazine, University of Toronto, Spring 2007
- <http://www.rotman.utoronto.ca/news/magazine.htm>

IT Risk Management



- CrossTalk – The Journal of Defense Software Engineering, February 2005
- <http://www.stsc.hill.af.mil/crosstalk/>

Development Risk Management



- Dorset House, 2003
- Title from *The Cat in the Hat Songbook*, by Dr. Seuss
 - Uncle Terwilliger “creeps down our back stairs, / sneaks out of our house to go waltzing with bears”

Software Engineering Institute



Technical Report
CMU/SEI-93-TR-6
ESC-TR-93-183
June 1993

Taxonomy-Based Risk Identification

Marvin J. Carr
Suresh L. Konda
Ira Monarch
F. Carol Ulrich



**Carnegie Mellon
Software Engineering Institute**
Pittsburgh, PA 15213-3890

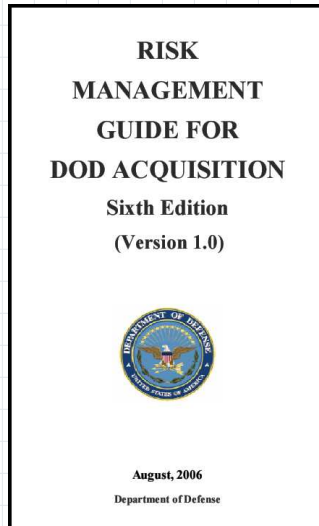
A Taxonomy of Operational Risks

CMU/SEI-2005-TN-036

Brian P. Gallagher
Pamela J. Case
Rita C. Creel
Susan Kushner
Ray C. Williams

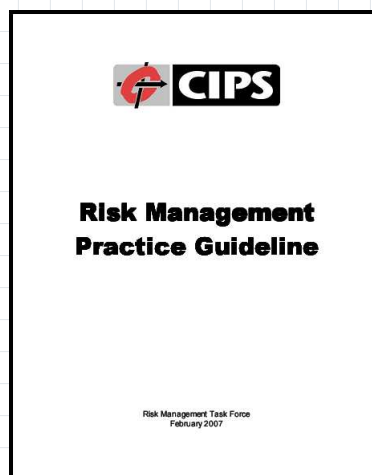
<http://www.sei.cmu.edu>

Acquisition Risk

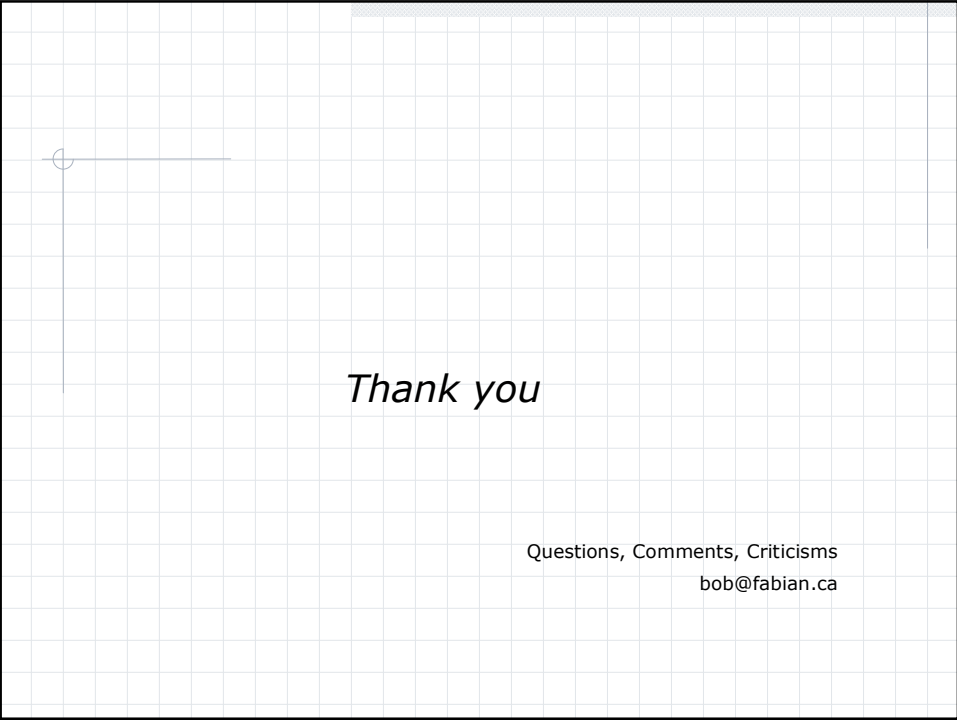


- It's not just development and operations
- Acquisition risk of growing importance
- <http://www.sei.cmu.edu/risk/>

Official CIPS Position



- <http://www.cips.ca>



Thank you

Questions, Comments, Criticisms
bob@fabian.ca