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
• 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
• 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
• 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

- Establish Risk Context
- Event Identification
- Risk Assessment
- Risk Response
- Maintain & Monitor Plan

Communicate
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

- Judgement – individuals/groups use their best judgement

1. Scenarios – examine qualitatively different alternatives
2. Models – formally model the activities under review
3. 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

#### Table: Risk Impact Rating

<table>
<thead>
<tr>
<th>Impact on Other Teams</th>
<th>Schedule</th>
<th>Cost Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unacceptable</td>
<td>Major</td>
<td>&gt; 10%</td>
</tr>
<tr>
<td>Acceptable - No Margin</td>
<td>Minor</td>
<td>5 - 7%</td>
</tr>
<tr>
<td>Acceptable - No Margin</td>
<td>Critical Path Impacted</td>
<td>5%</td>
</tr>
<tr>
<td>Notable to Meet Needed Dates</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

#### Diagram: Risk Assessment Guide

- **Level of Technical Performance**
  - 5: Minimal or No Impact
  - 4: Acceptable with Some Reduction in Margin
  - 3: Acceptable with Significant Reduction in Margin
  - 2: Moderate - Key Milestone - Notable to Meet Needed Dates
  - 1: Minimal or No Impact

- **Consequence**
  - Unacceptable
  - Cannot Achieve Key Team of Major Project Milestone
  - Schedule: May be 7 - 10%
  - Cost Impact: 5 - 7%

- **Probability**
  - Level of Likelihood Risk Will Happen
    - a: Minimal / Remote
    - b: Small / Likely
    - c: Probable / Likely
    - d: Large / Highly Likely
    - e: Significant / Near Certainty

The diagram illustrates the assessment of risk impact rating based on the level of technical performance and consequence, with a grid for probability assessment.
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”
Acquisition Risk

- It’s not just development and operations
- Acquisition risk of growing importance
  - http://www.sei.cmu.edu/risk/
Official CIPS Position

Risk Management Practice Guideline

Risk Management Task Force
February 2007

• http://www.cips.ca
Thank you

Questions, Comments, Criticisms
bob@fabian.ca