Risk Assessment Practicum

Dr. AT Shuldiner
Basel Consulting

Risk Assessment Defined

A document describing a set of risks applicable to a given product or operation. It should:

- Define the various operational and technical areas of concern (e.g., “Access Control” or “Business Continuity Management”)
- Enumerate the relevant risks and sort them into at least two categories: controlled risks (i.e., risks that are either minimized or hedged) and accepted risks
- Assign responsibility for on-going control or acceptance of each identified risk

Dr. AT Shuldiner
alec@baselconsulting.com

The Basics

- State type of risk assessment
- Complex document with multiple audiences: use version #s for tracking
- *Don't generate more risk!*
  - Limit distribution and track carefully
  - Recall & destroy all copies
  - Emphasize security from the start

Dr. AT Shuldiner
alec@baselconsulting.com

Introductory Material

- Document has a diverse audience, therefore:
  - Explain type of risk being assessed
  - Explain scope of assessment, especially what is *not* covered
  - Explain project or area of concern
- Define risk areas (often pre-defined)
- Define controls (1-10, red/yellow/green, statistical, etc.); note: not all risks can be controlled
- Executive summary defining overall risk status: *leave no excuse for management ignorance*

Dr. AT Shuldiner
alec@baselconsulting.com

Example: Business Continuity Management

- Statement of Risk: normal language, avoid specifics, no precise estimate of potential harm needed but possibly note worst case scenario
- General Controls: what is your Plan A?
- Control matrix: risks are enumerated, grouped, assigned, specific; controlled risks assigned to a *role*, otherwise assigned to a *name*
- Accepted Risks: must be precisely described; state both probability & consequences

Dr. AT Shuldiner
alec@baselconsulting.com

Statement of Acceptance of Risks

Always some risks accepted, but:

- Each accepted risk must be accepted by a specific individual (name not role)
- This individual must have proper authority and competence to do so
- Very unlikely that one person can properly judge acceptability of all risks
- Accepted risks must also be explained!

Dr. AT Shuldiner
alec@baselconsulting.com

What Makes a Good Risk Assessment?

- A living document: reflects changes in project & internal/external environments
- Responsibility unambiguously assigned: no responsibility, no motivation to improve
- Beware packaged RAs: rote checklists, “precise” probability assignments, RAs which lack proof that the author(s) understand the project
- Don’t forget to evaluate your suppliers’ RAs: no written RA, no real understanding of risk!

Dr. AT Shuldiner
alec@baselconsulting.com