Introducing the Gartner Risk Assessment Method

Christian Byrnes
6 November 2008
Risk assessment (RA): it's not just a CISO opinion anymore.

Any process must be brief, effective and efficient if we want business involvement.

RA is the other half of governance.

Applying Delphi principles to the RA process solves some difficult problems.
Risk Assessment and Risk Management

Establish context

Define contextual risk criteria to guide risk assessment

**Evaluation criteria:**
- Definition of acceptable risk
- Statement of materiality
- Strategic goals
- Compliance requirements
- Stakeholder requirements
- Etc.

**Define:**
- Impact tables
- Control maturity
- Risk catalogue, register

Define contextual risk criteria to guide risk assessment

Identify and analyze risk

Evaluate and prioritize risks

Develop treatment plan

Implement plans

Risk Register

Controls Assessment
**What Is GRAM?**

**Identify risks**
- An asset owner defines requirements.
- An assessor defines a scenario for review.

**Assess risks**
- Threats
- Probability/impact
- Controls
- Description

**Delphi method**
- Subject matter experts review scenarios
- Consolidation and sanitized responses reviewed

**Develop scenario**
- Predefined evaluation criteria used

**Recommend treatment**
- Residual risk statement
- Risk treatment proposal

**Treat risks**
- Develop treatment plan

An asset owner defines requirements, and an assessor defines a scenario for review. The Delphi method is applied, wherein subject matter experts review predefined evaluation criteria used. After final consolidation, the assessor prepares a residual risk statement and a risk treatment proposal.**
Identifying Risks Using GRAM

**Asset**
- Information
- Application
- Process
- Platform etc.

The assessor engages with the asset owner to scope the assessment.

**Scenario**

The assessor develops the scenario from threats, impacts, controls. The assessor is a member of the security team.

**Threat table**
Table listing typical threats:
- DoS
- Worm
- Theft of sensitive information
- Etc.

**Impact table**
Table listing impacts derived from a detailed impact reference table.

**Current control maturity**
Table of controls and control maturity. (Obtained from control self-assessment and vulnerability assessments)

These tables are predefined and reused for ongoing, consistent risk assessment.
Scenarios for Risk Identification

1. Assessor, asset and asset owner are known.
2. Assessor:
   - Has discussed threats with the asset owner
   - Develops a scenario for the most likely threats
   - Appoints review team and administrator
3. Scenario contents:
   - Scope, objectives and deliverable
   - A description of the asset and the context of the asset
   - Threat being assessed
   - Current controls
   - Probability/impact graphs
   - Description of risk and rationale for probability and impact

Threat Table

<table>
<thead>
<tr>
<th>Threat</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS</td>
<td></td>
</tr>
<tr>
<td>Data theft</td>
<td></td>
</tr>
<tr>
<td>Worm</td>
<td></td>
</tr>
</tbody>
</table>

Impact reference table

<table>
<thead>
<tr>
<th>Impact</th>
<th>Extremely serious</th>
<th>Very serious</th>
<th>Serious</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>&gt;$100m</td>
<td>$50-$100m</td>
<td>&lt;$25-$50m</td>
</tr>
<tr>
<td>Reputation</td>
<td>International publicity</td>
<td>National publicity</td>
<td></td>
</tr>
<tr>
<td>Disclosure</td>
<td>Penalties &gt;$100m</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Scenario Graphs — The Time Factor

Scenario:
Intentional disclosure of client data by employee to a competitor

Example impacts:
1 = Disruption to operations
2 = Loss of existing business
3 = Legal consequences
4 = Reputational harm

Multiple graphs are drawn using a future time frame to establish where and when control of impacts is required.

For a given asset or a given threat, a range of impacts could occur.
Who Is Involved in the Assessment?

- Assessor (member of risk/security team)
- Process administrator

The composition of the review team will vary depending on the asset being assessed, but typically is a combination of:

- Security professional
- Asset owner
- IT specialist
- SME(s) who understand the business and the asset

- Review team focuses on analyzing risk
- Administrator consolidates and distributes responses after each round
- Assessor facilitates process and engages with the asset owner
Using the Delphi Method to Analyze and Evaluate the Risks

The Delphi Method:

- A panel of experts individually review the scenarios in three rounds
- Results are consolidated after each round and redistributed to the panel
- Panel members review/revise their responses considering the group responses until convergence, if not consensus, is achieved

| Pass 1: Scenario evaluation | • Distribute scenarios with questions to team for review and response  
|=|• Consolidate responses from Pass 1 |
| Pass 2: Risk modeling | • Distribute updated scenarios with questions relating to impacts and probabilities  
|=|• Consolidate responses from Pass 2 |
| Pass 3: Controls review | • Distribute updated scenarios with questions relating to controls  
|=|• Consolidate responses from Pass 3 |
Start small – run GRAM against one asset with supportive owners.

Have a post-assessment review that is face to face if possible.

Start populating a risk register for senior management review.

Expand: more iterations using more people.

Elevate: assess larger asset groups, lines of business, etc.