GARTNER TELECONFERENCE

Introducing the Gartner Risk Assessment Method

Christian Byrnes

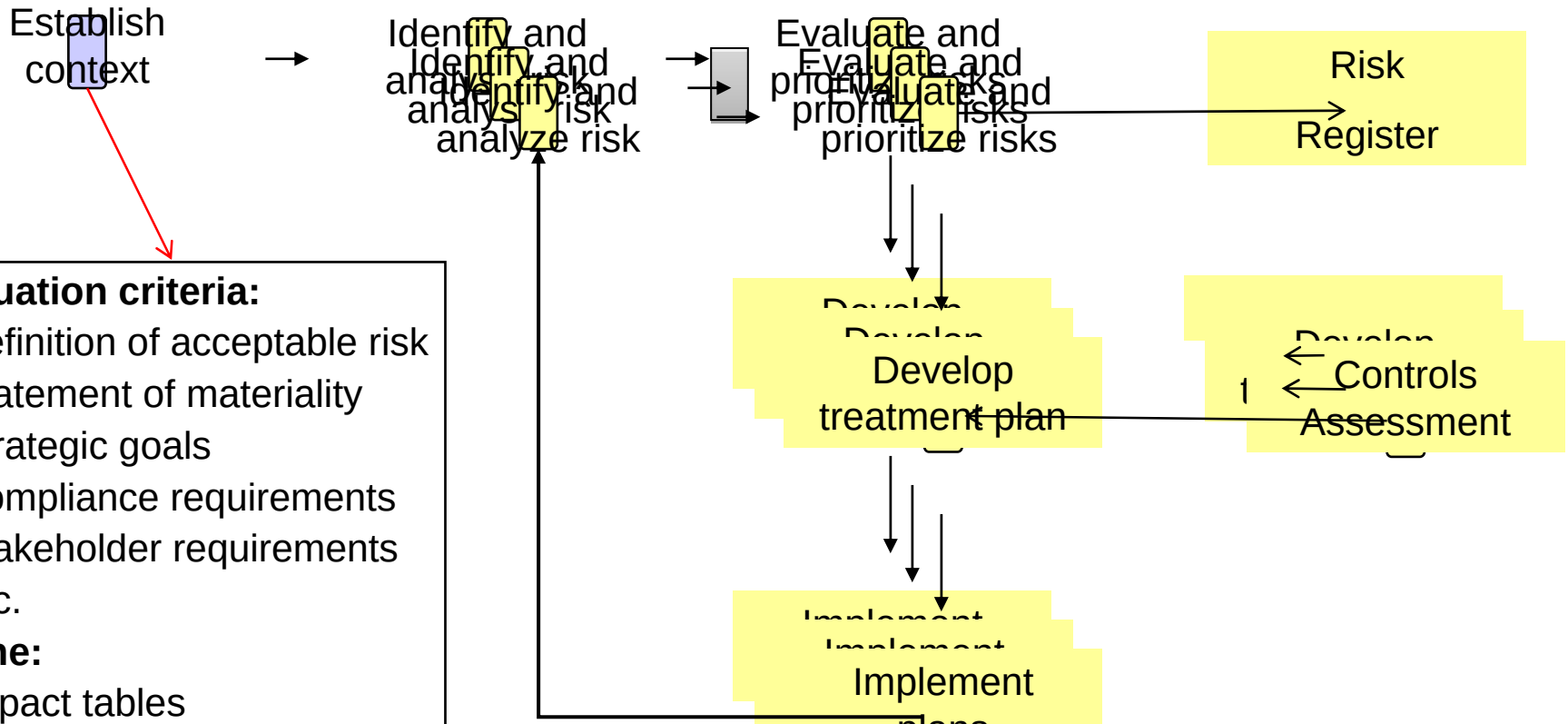
6 November 2008

Gartner®

The Little Secret of Most Practitioners

- 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



Evaluation criteria:

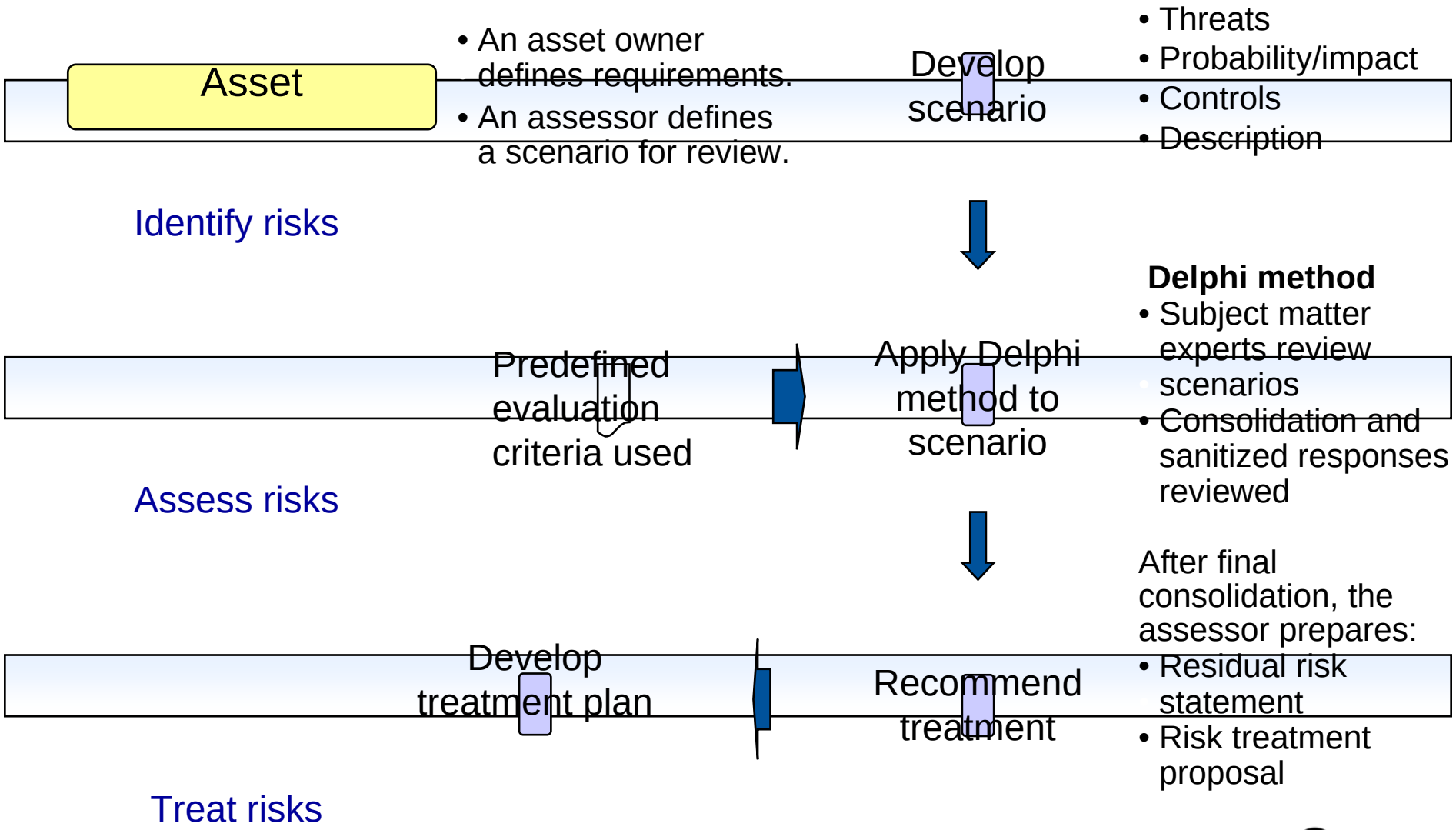
- Definition of acceptable risk
- Statement of materiality
- Strategic goals
- Compliance requirements
- Stakeholder requirements
- Etc.

Define:

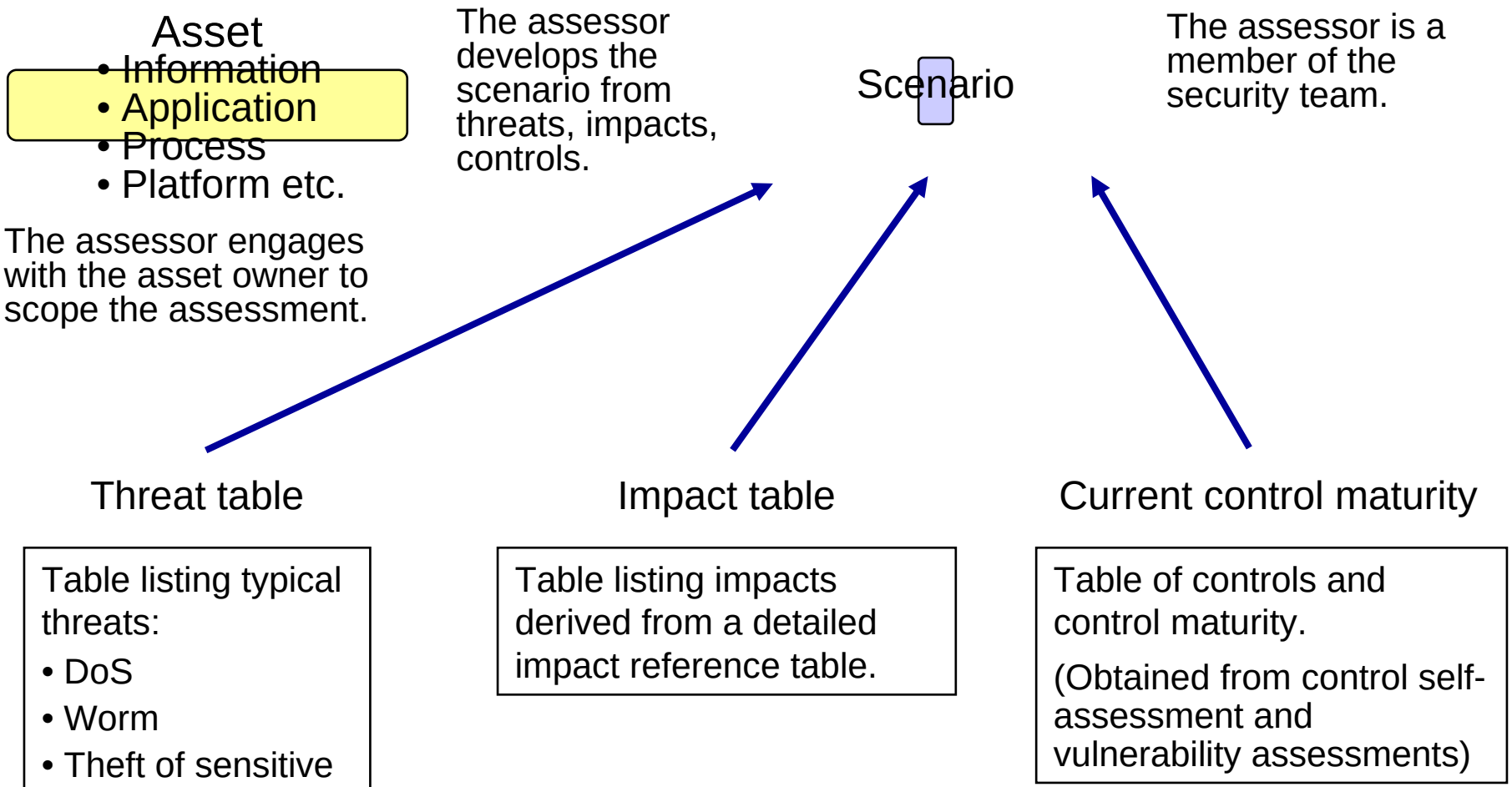
- Impact tables
- Control maturity
- Risk catalogue, register

Define contextual risk criteria to guide risk assessment

What Is GRAM?



Identifying Risks Using GRAM



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

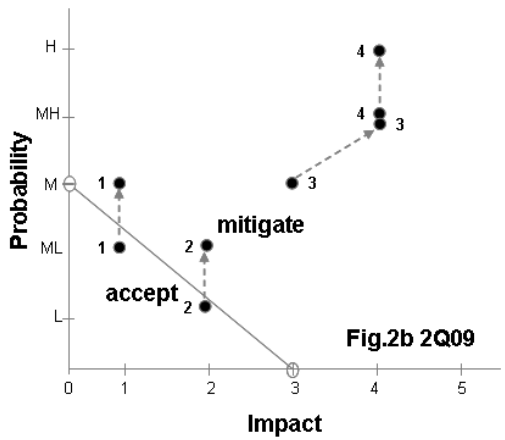
Scenarios for Risk Identification

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
DoS
Data theft
Worm

Impact reference table

	Extremely serious	Very serious	Serious
Financial	>$100m	$50-$100m	$25-$50m
Reputation	International publicity	National publicity	
Disclosure	Penalties >$100m		



Gartner

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

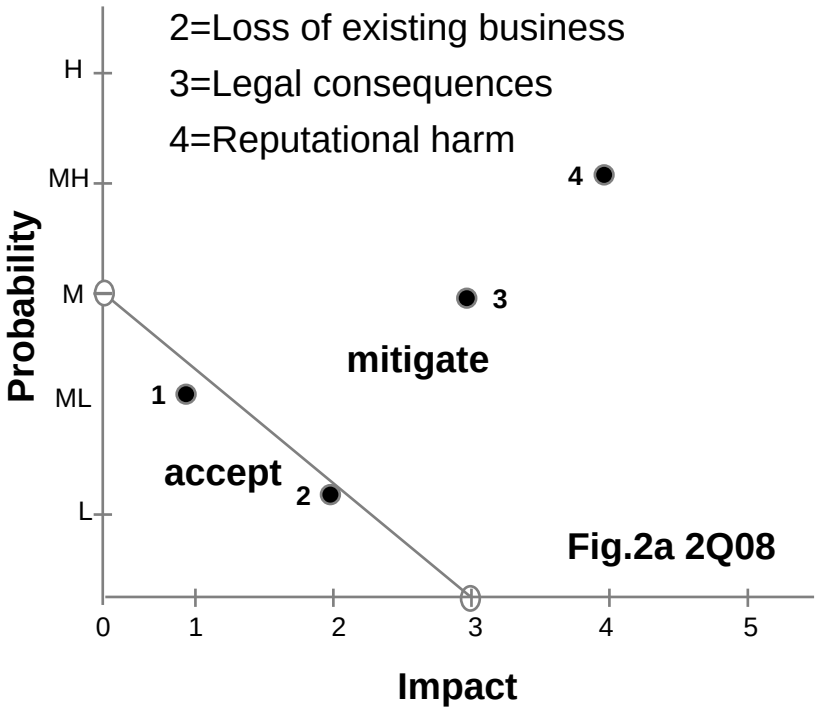


Fig.2a 2Q08

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

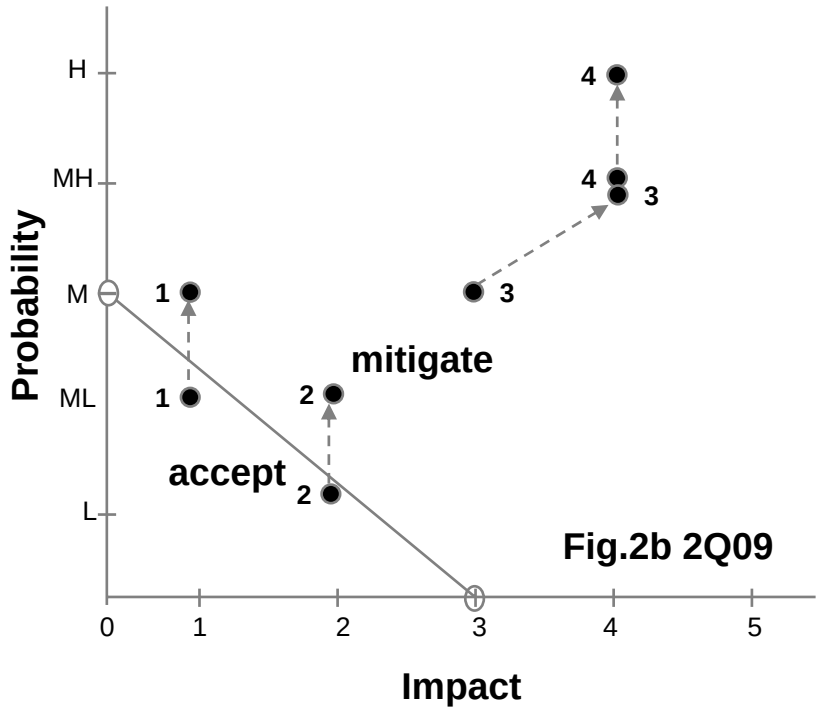


Fig.2b 2Q09

For a given asset or a given threat, a range of impacts could occur.

Gartner

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

Introducing GRAM

- 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.