

# Business Risk View

» Autor  
Marcos Sêmola  
marcos@semola.com.br  
Palestra Base 2006

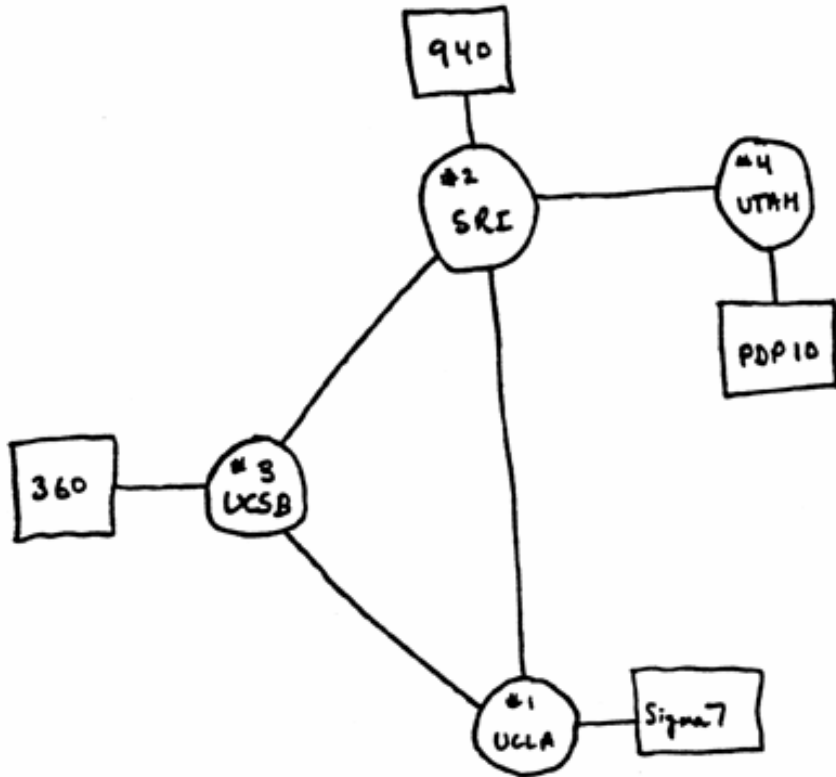
# Agenda

- » Information Age and New Business Risk Component
- » Info Risk Impacts
- » Info Risk
  - » Attributes
  - » Equation
  - » Lifecycle
  - » Composition
  - » Dynamism
  - » Source
  - » Reason
  - » Evolution
- » Info Risk Governance, Management and Assessment
- » Info Sec Control Maturity

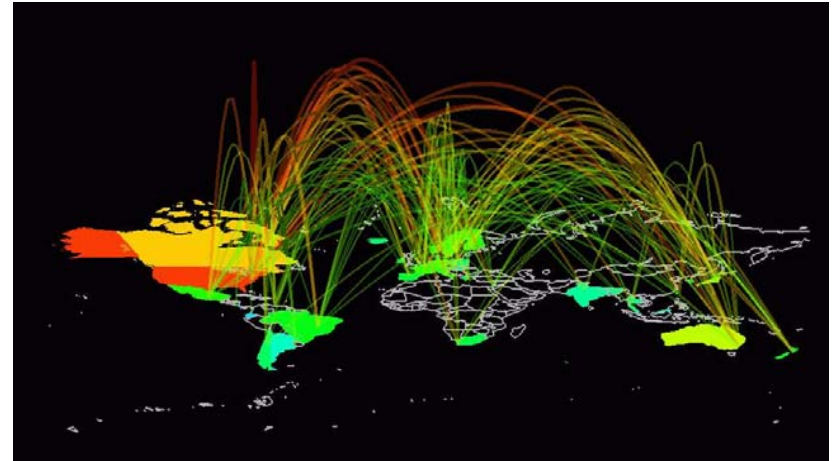
# Information Age

## Connectivity, Capillarity and Exposition

» Internet 1967

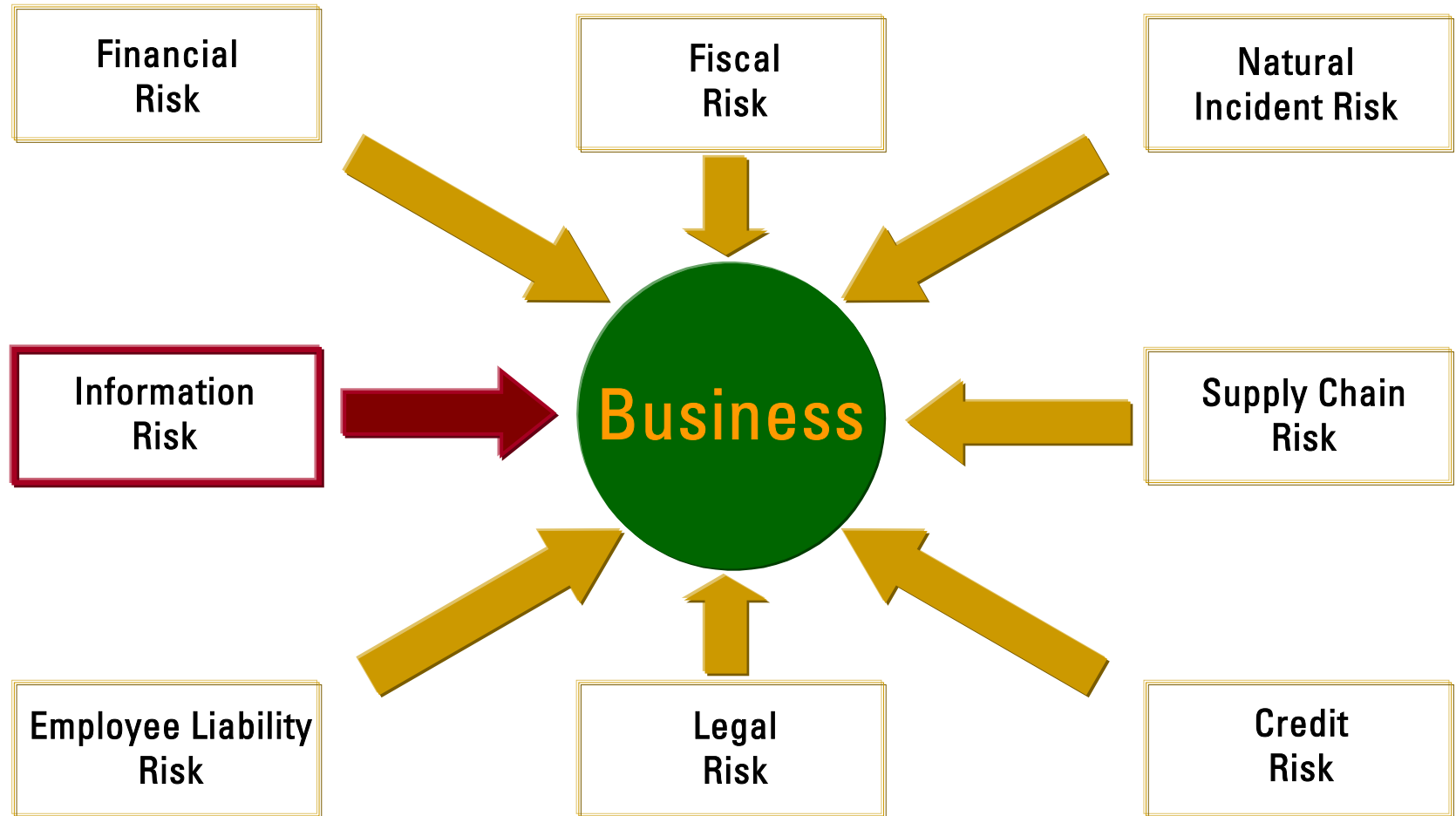


» Internet 2006





# New Business Risk Component

## Information Risk



# Info Risk Impacts

## Business Perspective Levels

- » Money Loss
  - » Opportunity Loss
  - » Liability
- 
- » Financial Fraud
  - » Legal Penalty
  - » Reputation Waste
  - » Identity Theft
  - » Client Data Privacy Loss
  - » Regulatory Non Compliant
  - » Downtime
  - » Time-to-Market Loss
  - » Unauthorized Access
  - » Business Secret Loss
  - » Productivity Loss
  - » Natural Catastrophes
  - » Terrorist Attacks
- 
- » Sarbanes Oxley Act
  - » Civil Contingencies Act 04
  - » FOIA
  - » EU Risk
  - » Basel II Principals
  - » MiFID
  - » FSA Handbook
  - » Prudential Handbook
  - » Companies Act
  - » NISCC
  - » HIPPA
  - » ...

# Info Risk Impacts

## Real Examples

### News headlines

#### February 2005

- Alistair Campbell gets into trouble for sending rude email to the BBC by mistake

#### February 2005

- Employee from Timber Taylors is sacked for sexually explicit emails

#### March 2005

- Harry Stonecipher, Boeing CEO, is forced to resign over email to mistress

#### June 2005

- Waterstone sacks employee over inappropriate blog comments



# Info Risk Impacts

## Real Examples

### News headlines

#### February 2006

"A computer virus attack forced a suspension of trading on the RTS FORTS futures market, classic market and the stock exchange," the Russian Trading System stock exchange said in a statement.

#### March 2006

- According to the Japanese press, information about 1500 individuals, related to police investigations was leaked from a virus-infected computer belonging to an Okayama Police investigator.
- According to the report, the leak occurred because the policeman was storing data about investigations on his personal computer. The PC was infected with an unnamed computer virus which is said to have enabled Winny users across Japan to access the sensitive information. The exposed data included the names of sex crime victims.

#### April 2006

- The failure of a Trend Micro Inc. employee to install his company's own antivirus software led to the uploading of some company reports to a popular Japanese peer-to-peer file-sharing network.

# Info Risk Impacts

## Real Examples

### What's the real cost of downtime?

Industry	Application	Ave cost per hour of downtime
Financial	Brokerage operations	\$7,840,000
Financial	Credit card sales	\$3,160,000
Media	Pay-per-view	\$183,000
Retail	Home shopping (TV)	\$137,000
Retail	Catalogue sales	\$109,000
Transportation	Airline reservations	\$108,000
Entertainment	Tele-ticket sales	\$83,000
Shipping	Package shipping	\$34,000
Financial	ATM Fees	\$18,000

Source: HEWLETT PACKARD



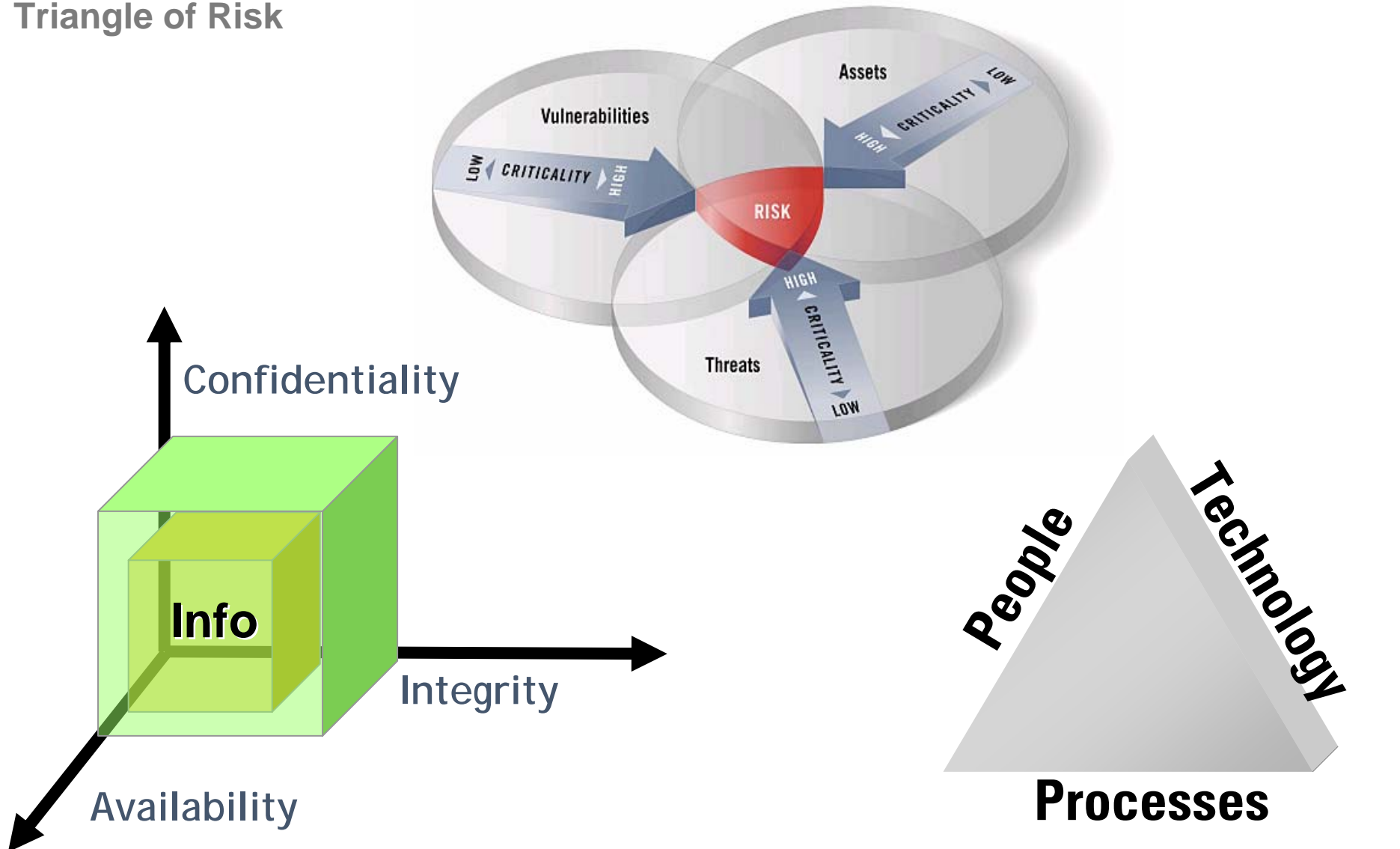
# Info Risk Impacts

## Real Examples



# Info Risk Attributes

## Triangle of Risk



# Info Risk Equation

Variables of risk

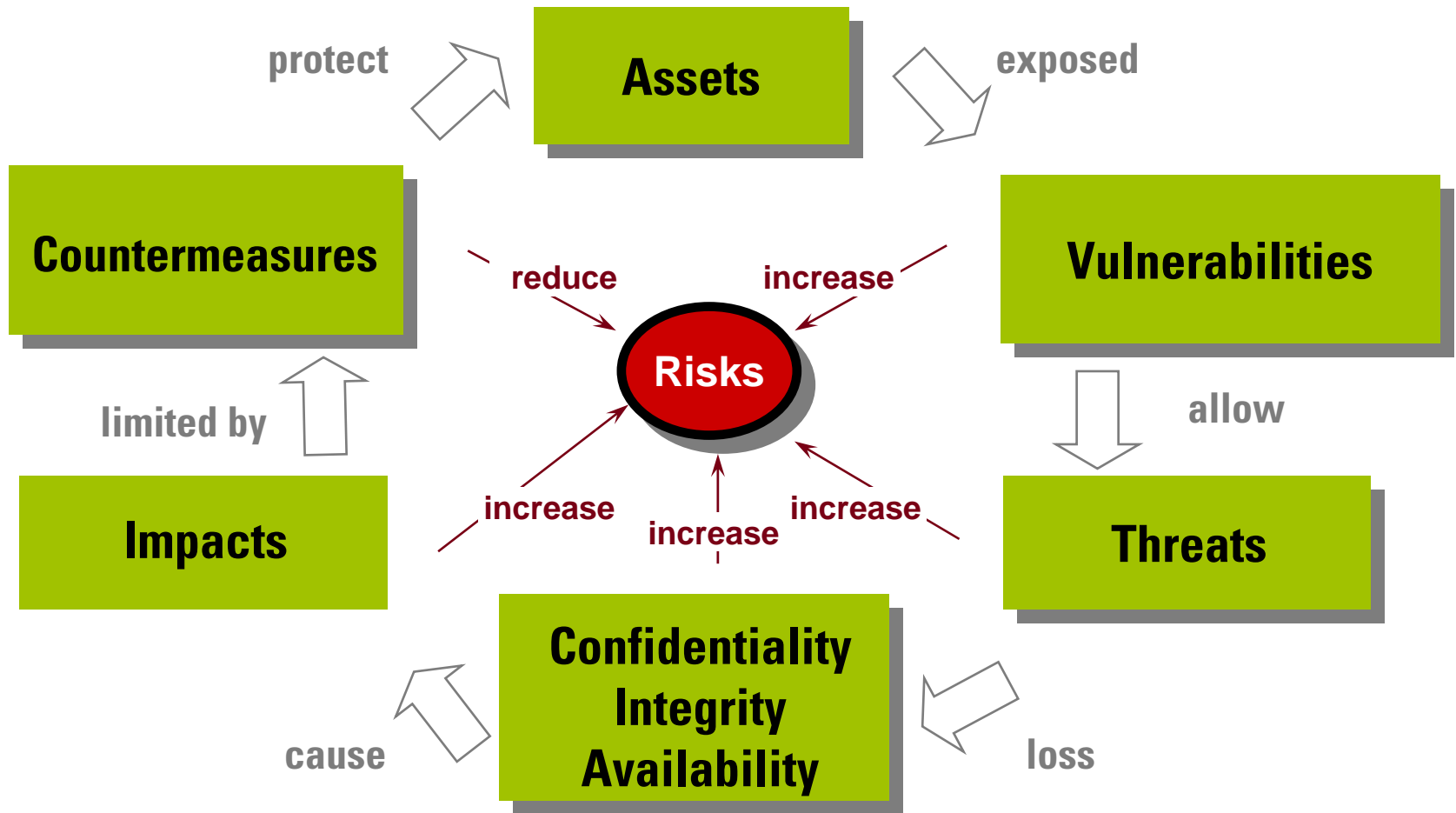
$$\text{Risk} = \frac{\text{Threats x Vulnerabilities}}{\text{Countermeasures}} \times \text{Asset Value}$$

## Risk Dimentions

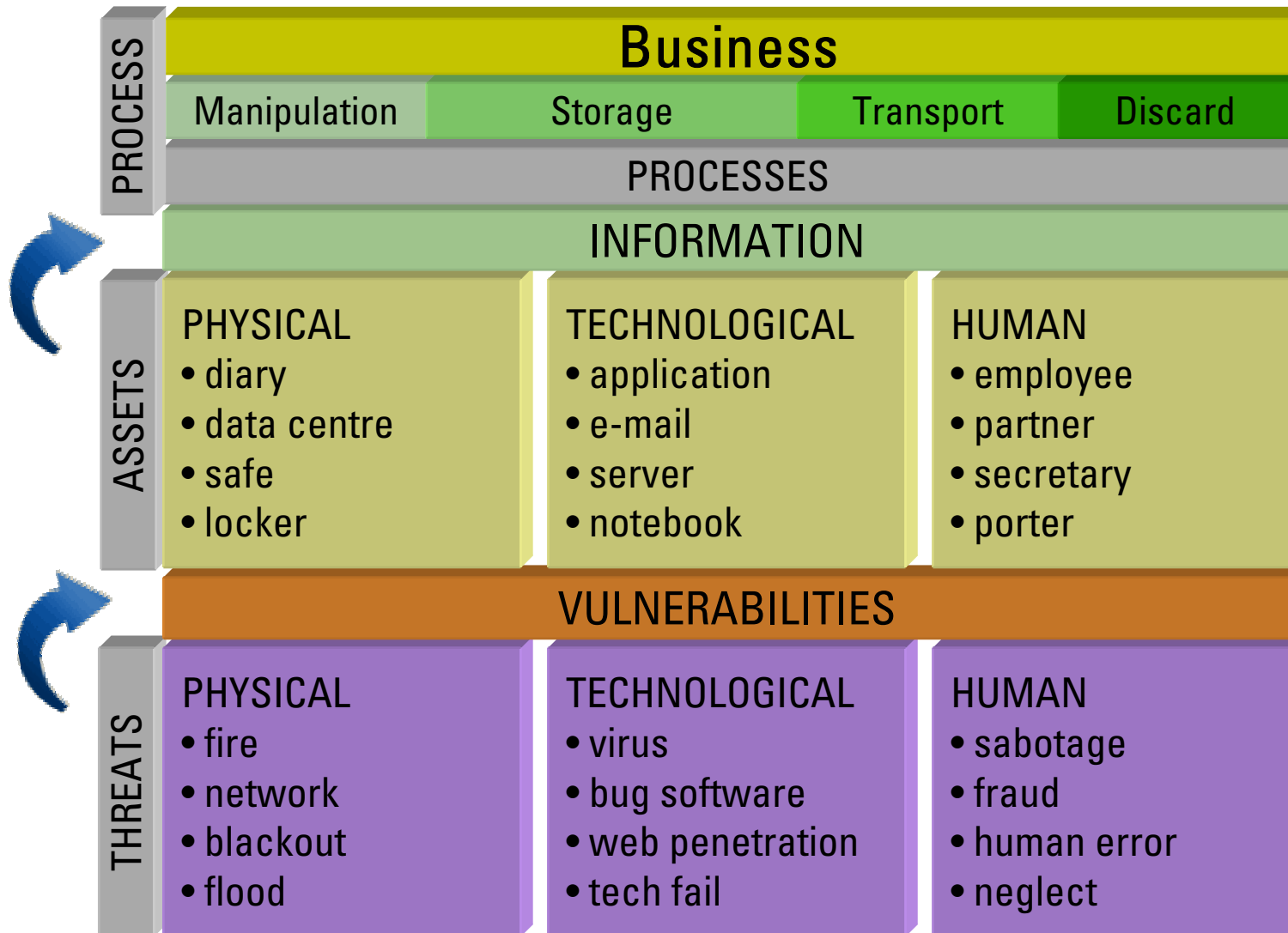
- Inherent Risk
- Present Risk
- Residual Risk

# Info Risk Lifecycle

Dynamic flow



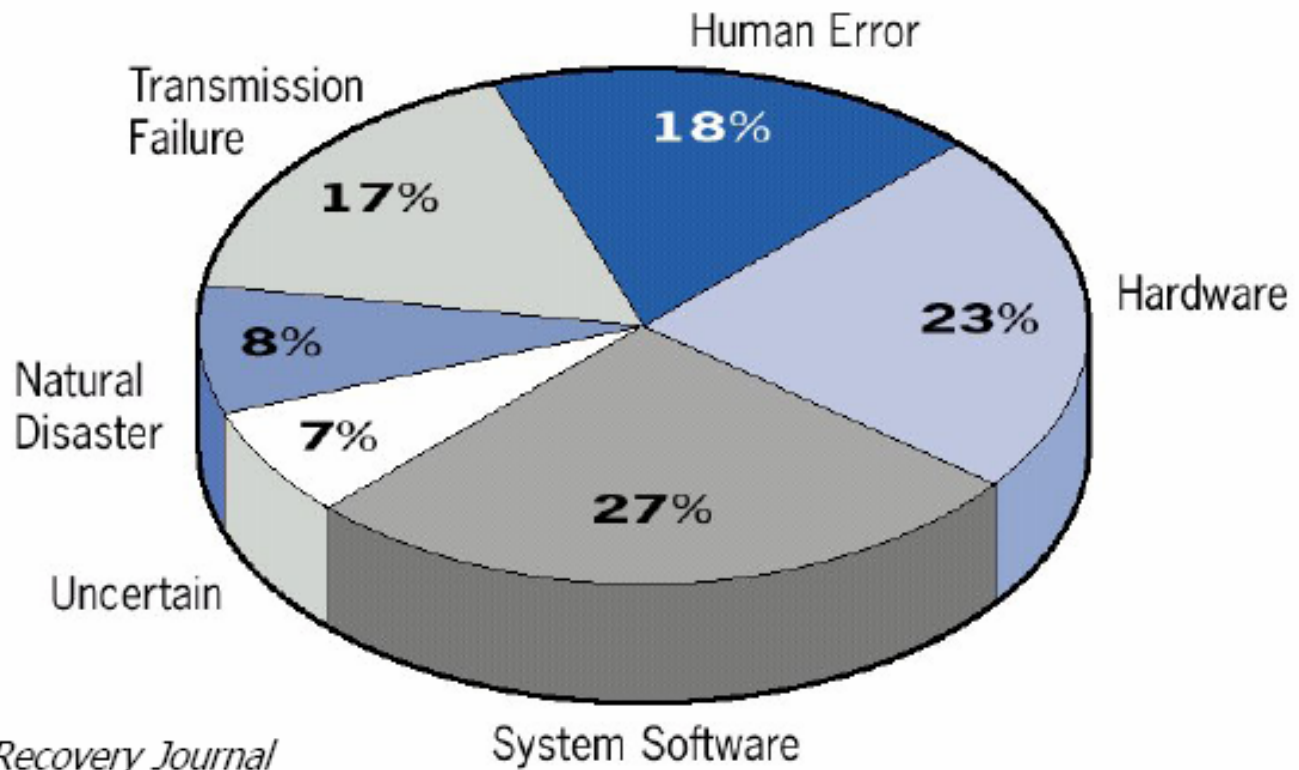
# Info Risk Composition



**THREATS** explore  
**VULNERABILITIES**  
present on **ASSETS**  
that keep **INFORMATION**,  
generating **RISK** and potential  
**IMPACTS** on **BUSINESSES** that can  
be mitigated by  
**COUNTERMEASURES**

# Info Risk Sources

## Research



*Fonte: Disaster Recovery Journal*

# Info Risk Reasons

## Research

- **45%\*** of companies hire new staff without running background checks
- **55%\*** of companies have no restrictions on use of Removable Media Devices
- **85%\*** of companies reported staff abuse of confidential information
- **71%\*\*** of companies faced computer security breaches within the past 12 months

\* DTI/Information Security Breaches Survey 2006

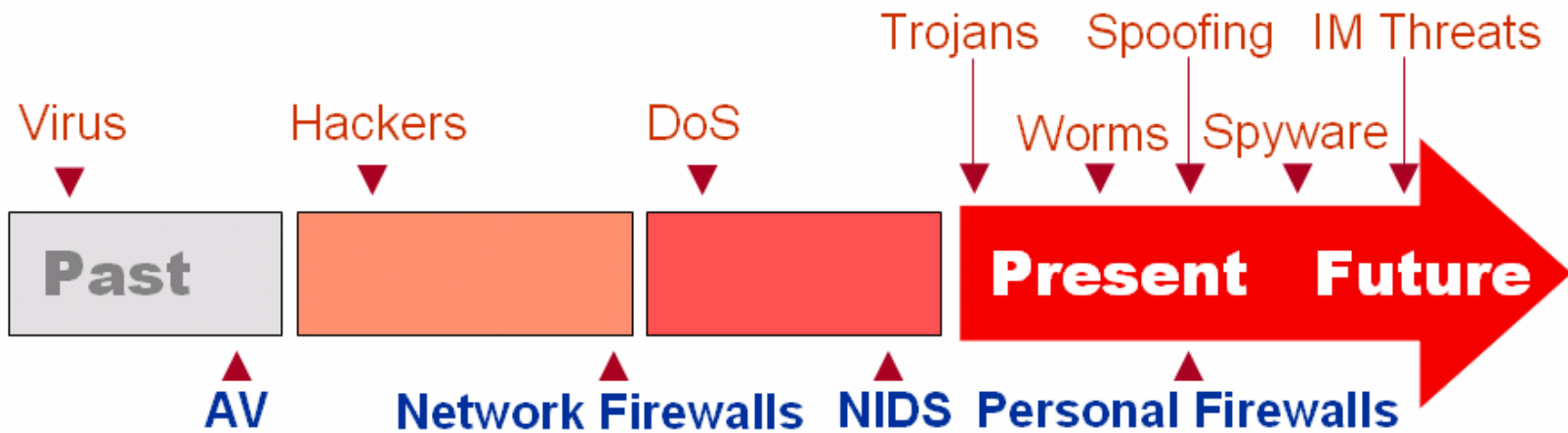
\*\* CSI/FBI Survey 2005



# Info Risk Evolution

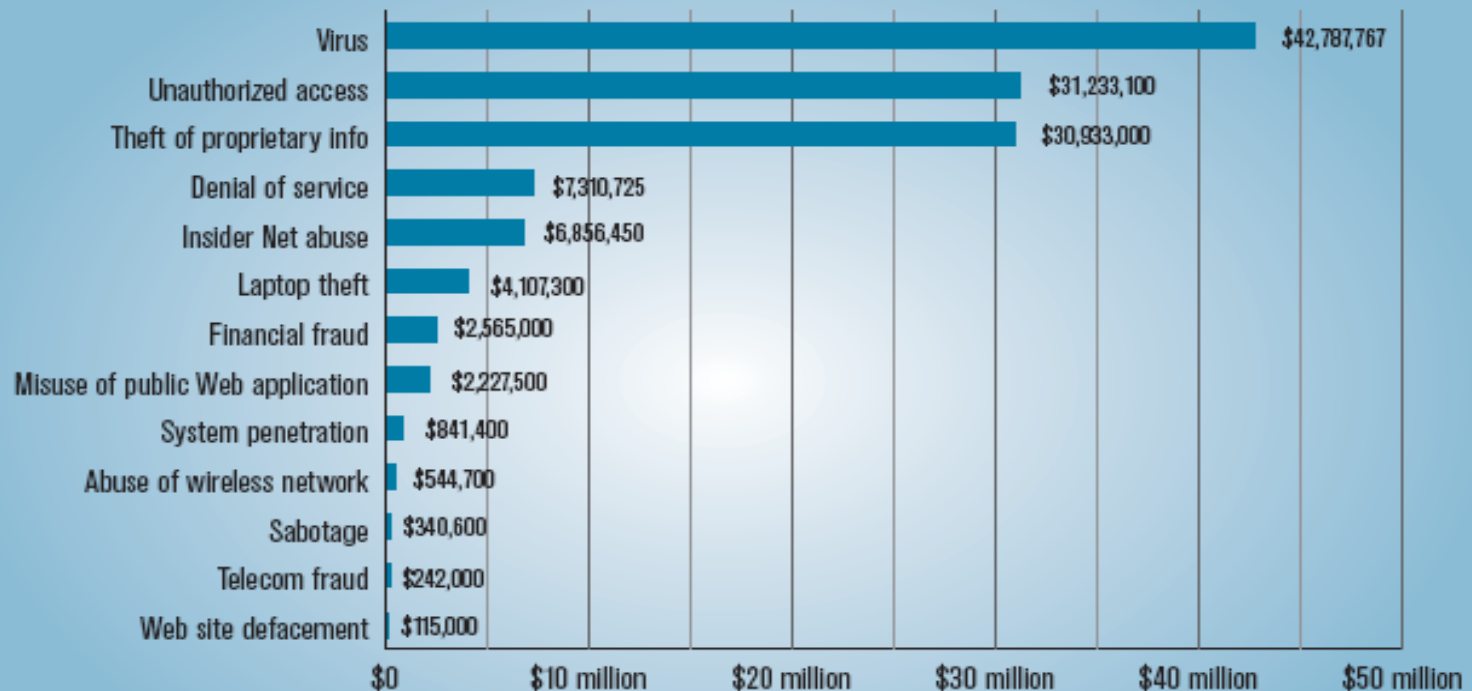
## Tech Perspective

### Sophisticated Threat Evolution



# Loss Sources through Info Risk

**Figure 16. Dollar Amount Losses by Type**



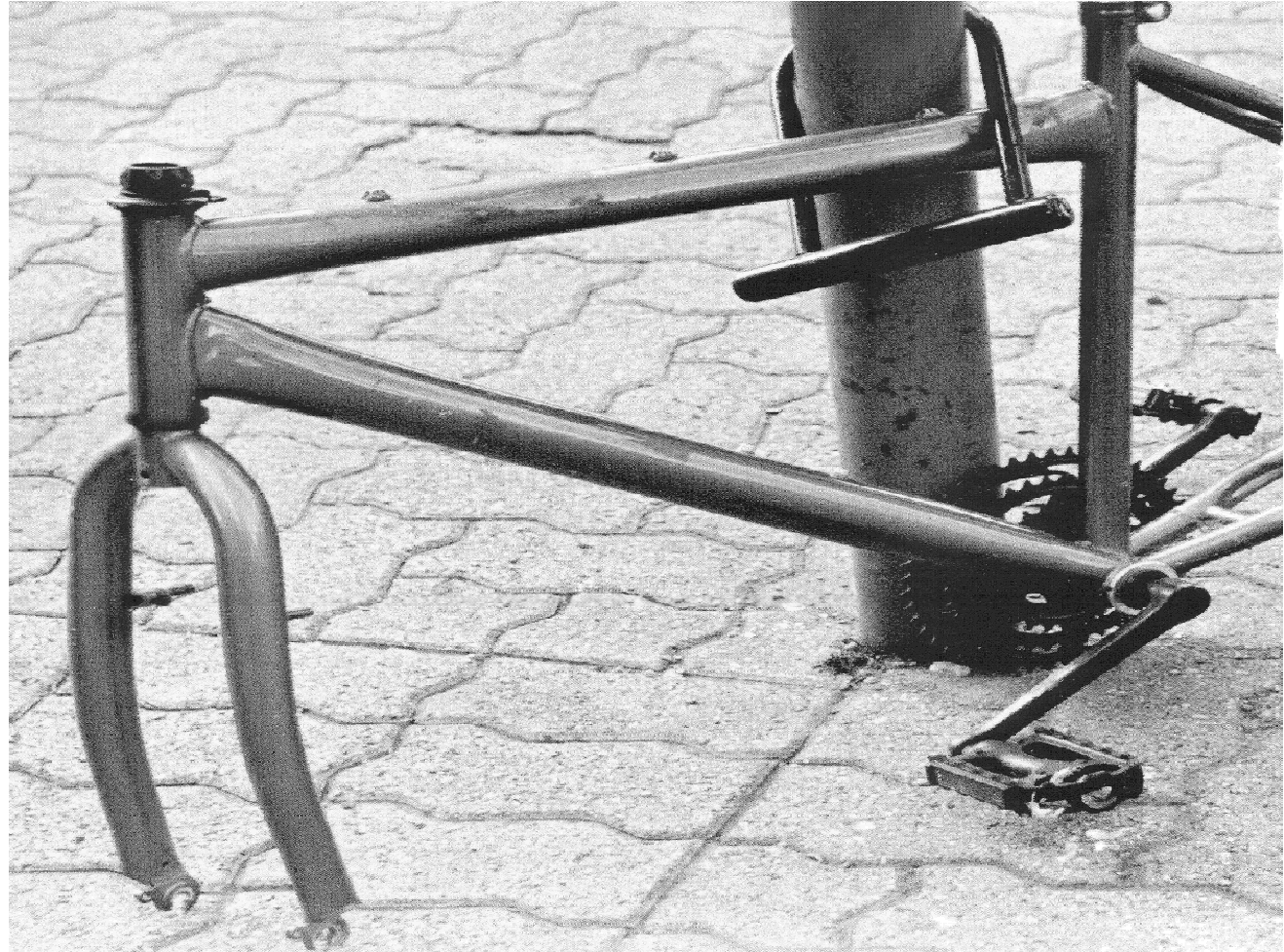
*Total Losses for 2005 were \$130,104,542*

CSI/FBI 2005 Computer Crime and Security Survey  
Source: Computer Security Institute

2005: 639 Respondents

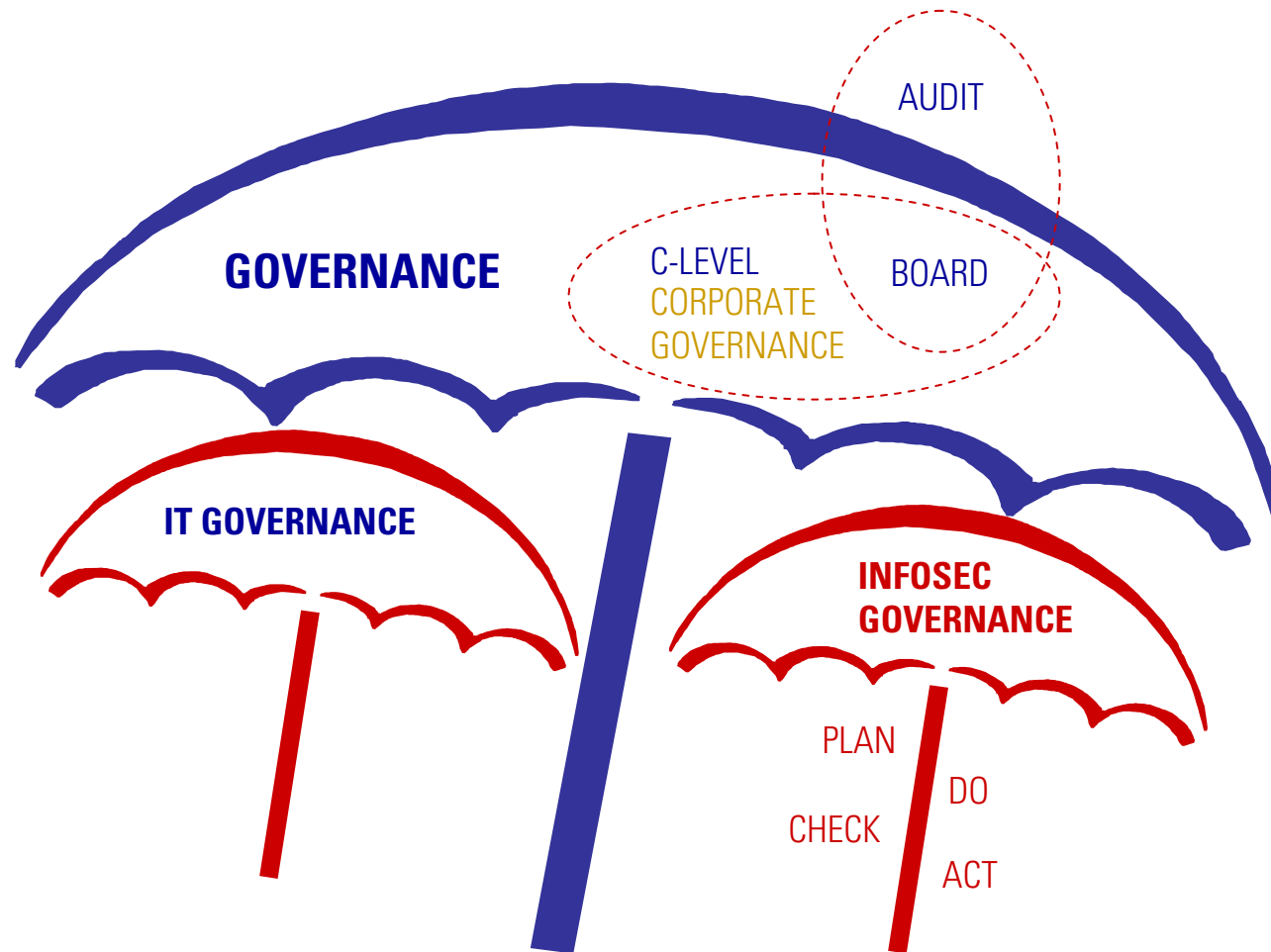
# Wrong Risk Approach Effect

Non integrated risk management view



# Info Risk Governance Approach

## Corporate View



# Business Priorities

## Gartner Research

and improve efficiency, relationships, improve competitiveness

### Top 10 Business and Technology Priorities in 2006

Gartner

Top 10 Business Priorities	Ranking	Top 10 Technology Priorities	Ranking
Business process improvement	1	Business Intelligence applications	1
Controlling enterprise operating costs	2	Security technologies	2
Attracting and growing customer relationships	3	Mobile workforce enablement	3
Improving competitive advantage	4	Collaboration technologies	4
Improving competitiveness	5	Customer sales and service	5
Using intelligence in products and services	6	Service Oriented Architectures (SOA)	6
Security breaches and disruptions	7	Workflow management	7
Revenue growth	8	Networking, voice and data communications	8
Faster innovation	9	Virtualization	9
Faster innovation and cycle times	10	Legacy application modernization	10

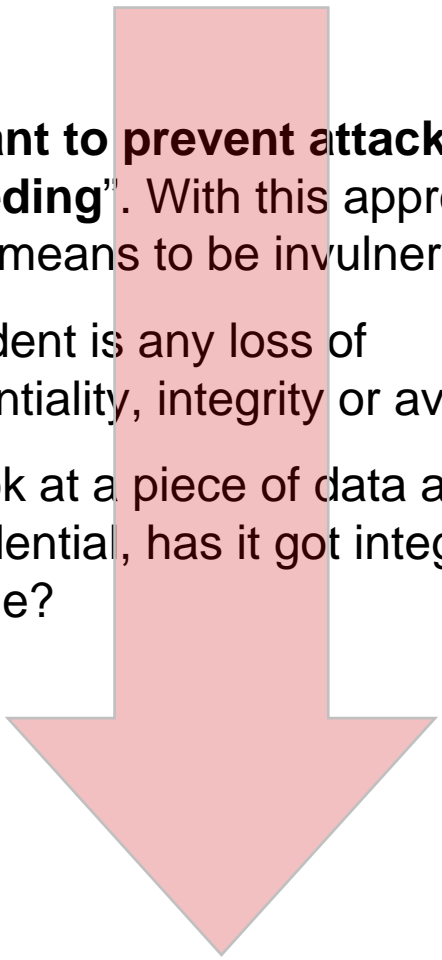
Source: Gartner EXP (January 2006)

CIOs are playing a leading role in business-foot

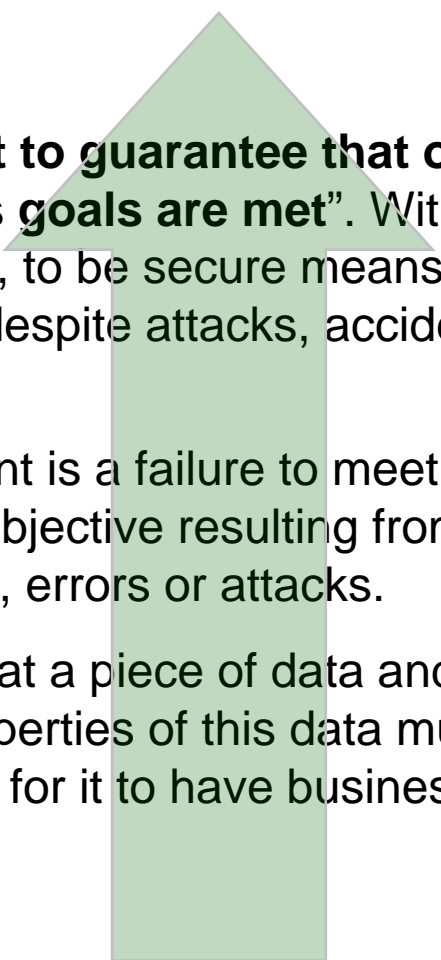
# Info Risk Management Approach Comparison

## Tech vs. Business Perspectives

### Tech Oriented

- 
- » “**We want to prevent attacks from succeeding**”. With this approach, to be secure means to be invulnerable.
  - » An incident is any loss of confidentiality, integrity or availability.
  - » You look at a piece of data and think: Is it confidential, has it got integrity, is it available?

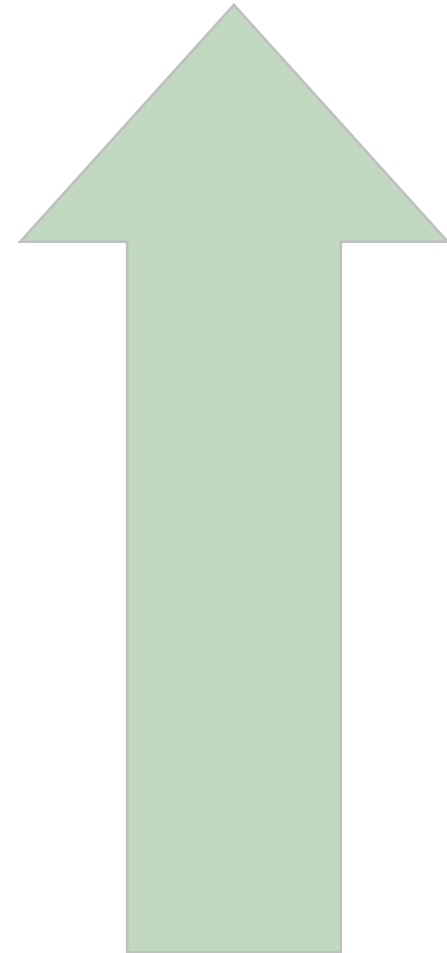
### Business Oriented

- 
- » “**We want to guarantee that our business goals are met**”. With this approach, to be secure means to be reliable, despite attacks, accidents and errors.
  - » An incident is a failure to meet a security objective resulting from accidents, errors or attacks.
  - » You look at a piece of data and think: What properties of this data must be protected for it to have business value?

# Info Risk Management Focus

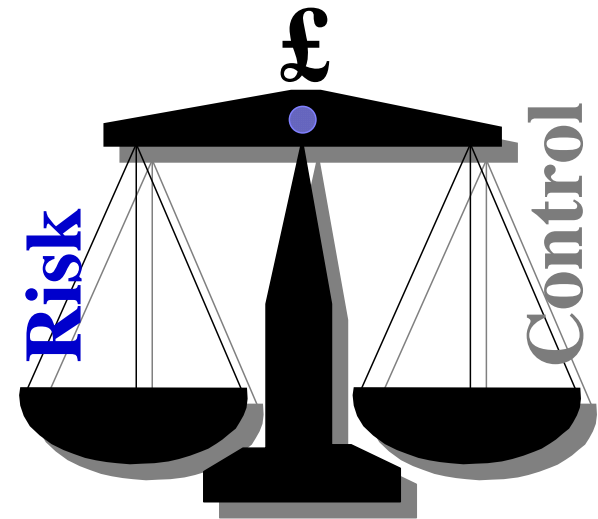
## Business Oriented

- » Business Objectives – Fundamental to the existence of an organization. Resilience depends on security objectives.
- » Security Objectives are derived from business objectives and specify the goals of the ISM.
- » Security Targets measure the achievement of security objectives in business terms.



# Business Risk Level vs. Infosec Investment

Approach balanced and compliant with business nature





# Info Risk Management System by ISO17799

## Risk Management

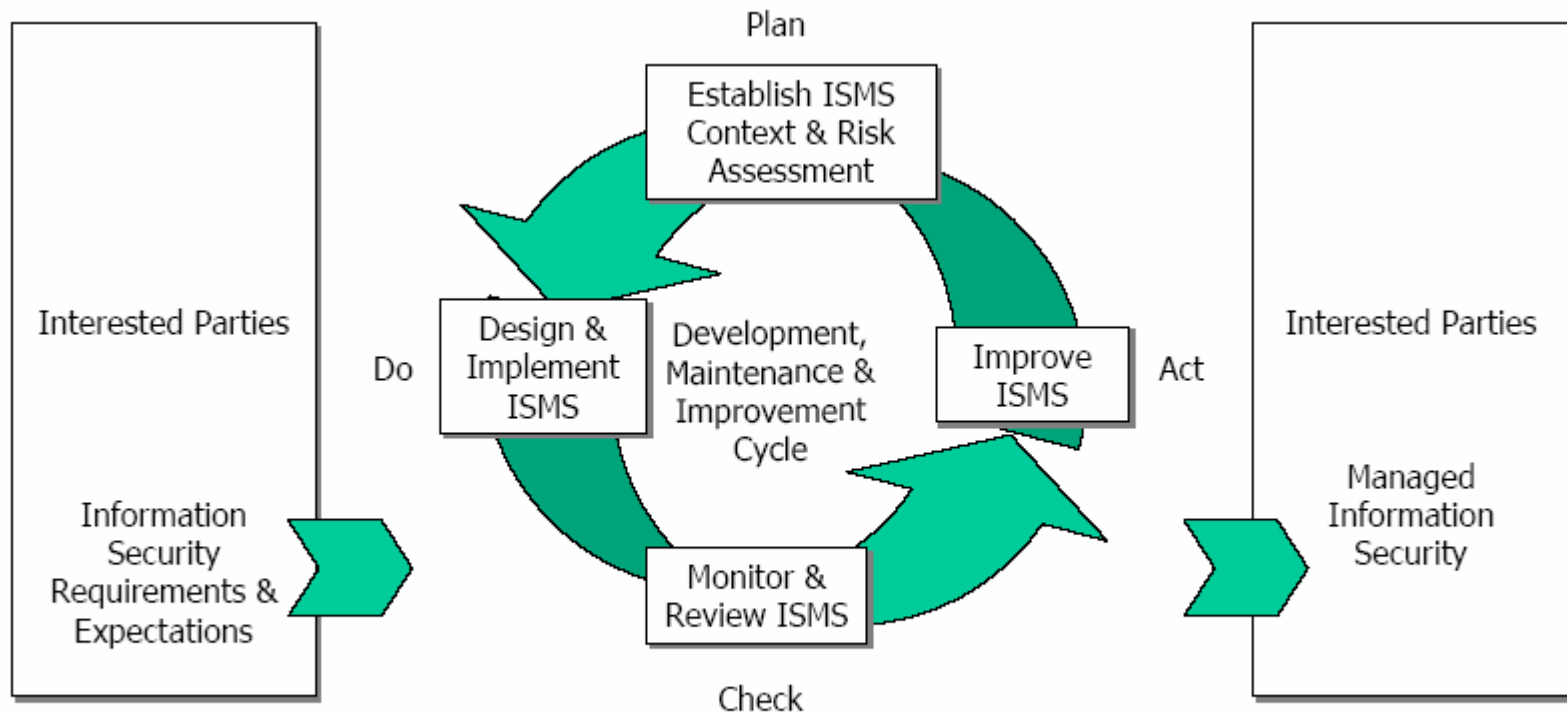
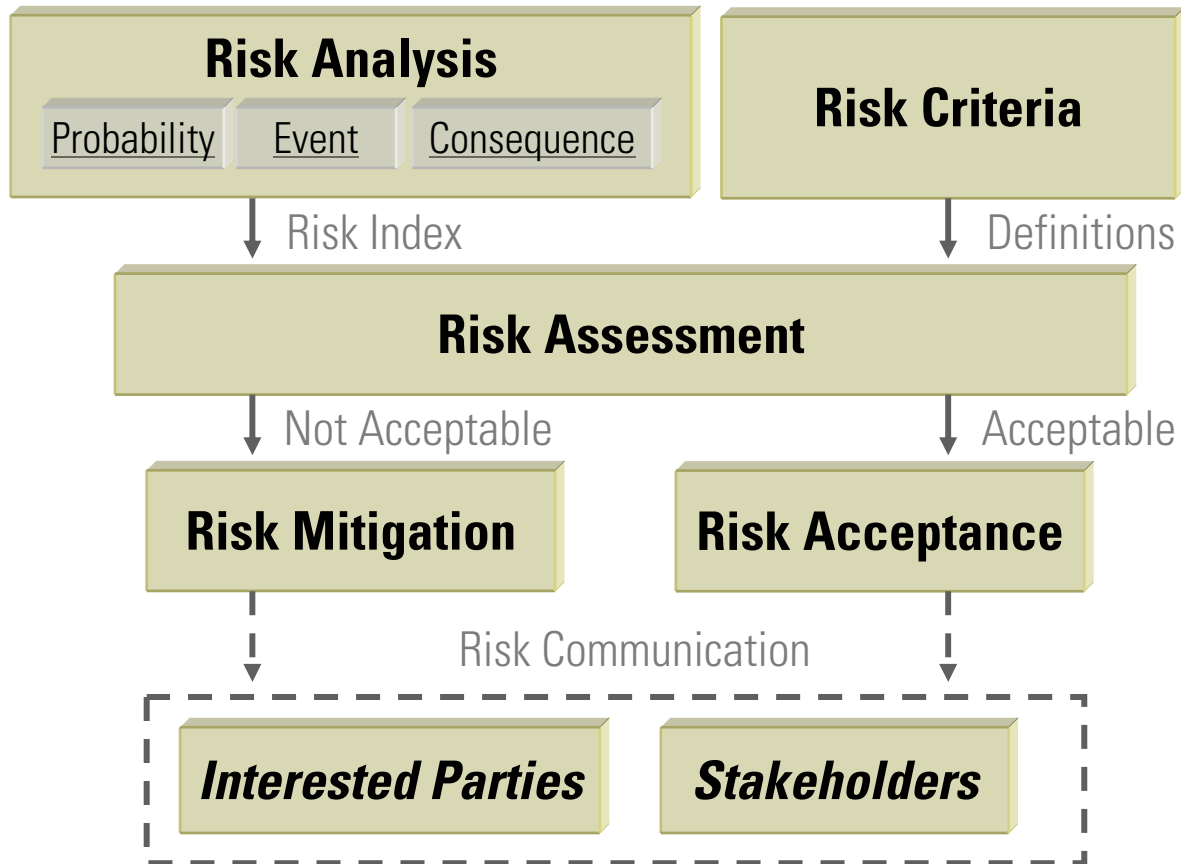


Figure 1 PDCA Process Model

# Info Risk Management based on ISO Guide 73

## Risk Governance

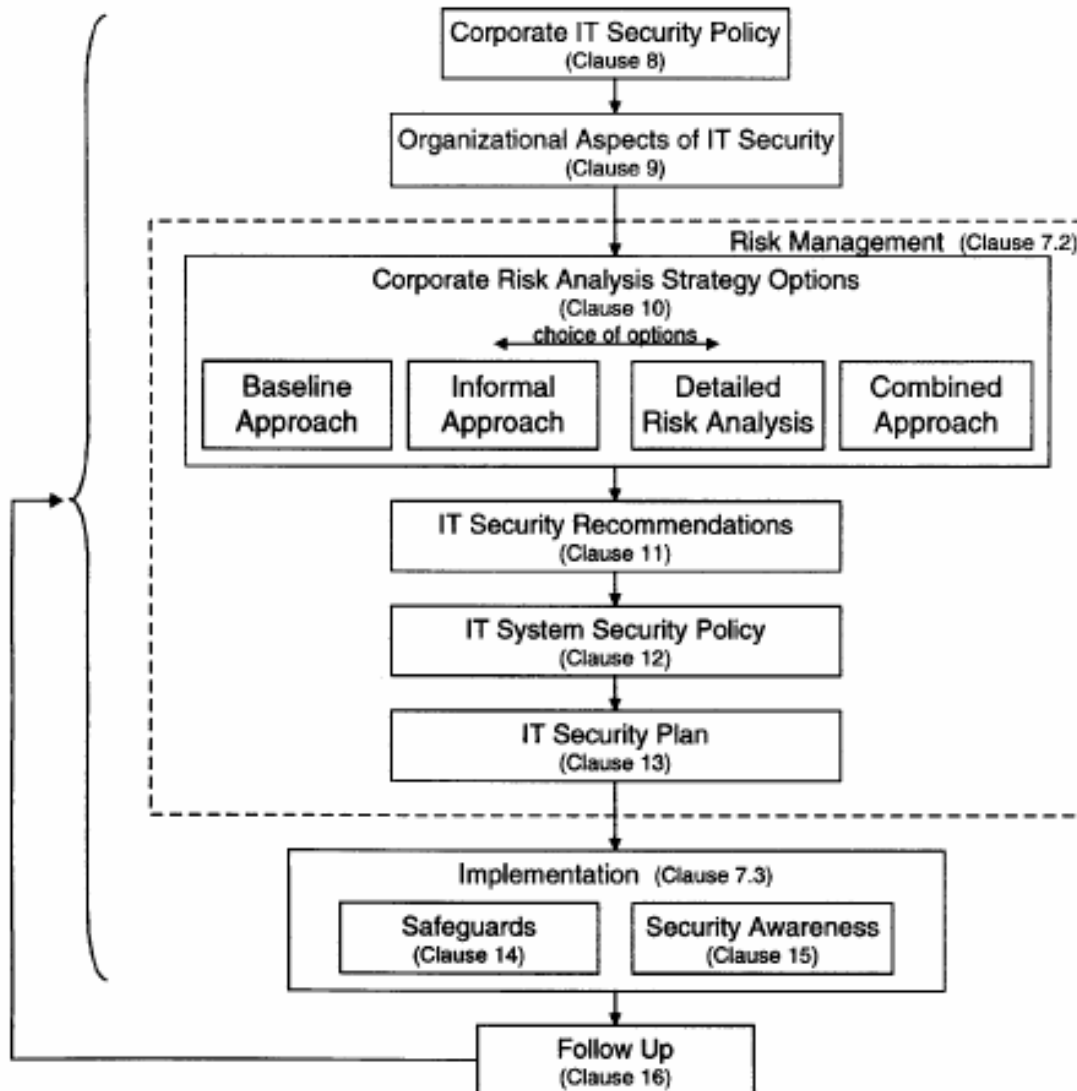


GUIDE 73

Risk management —  
Vocabulary — Guidelines for use  
in standards

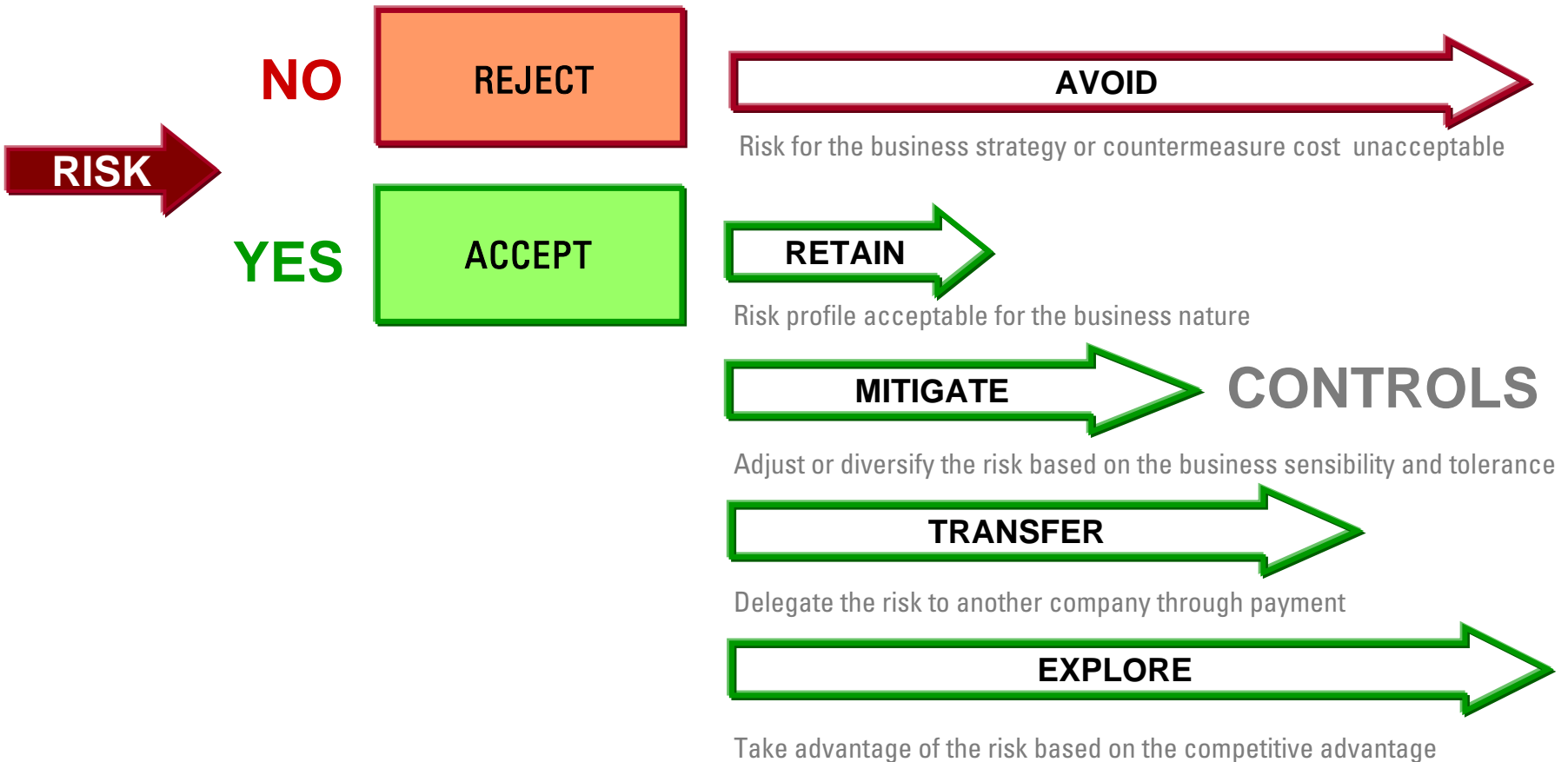
Management du risque —  
Vocabulaire — Principes  
directeurs pour l'utilisation dans  
les normes

# Info Risk Assessment based on ISO 13335



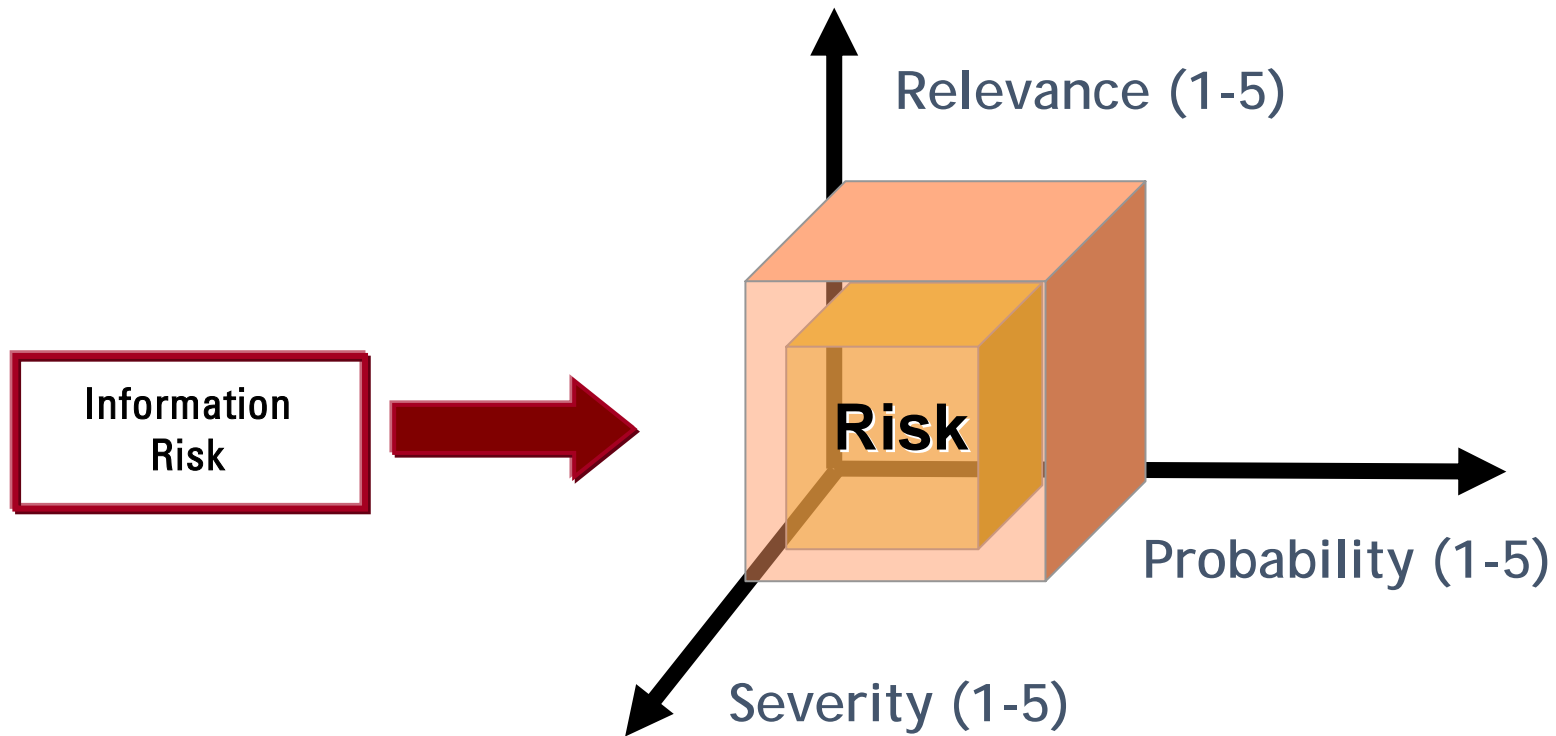
# Info Risk Management Approach

## Business Decision



# Info Risk Evaluation

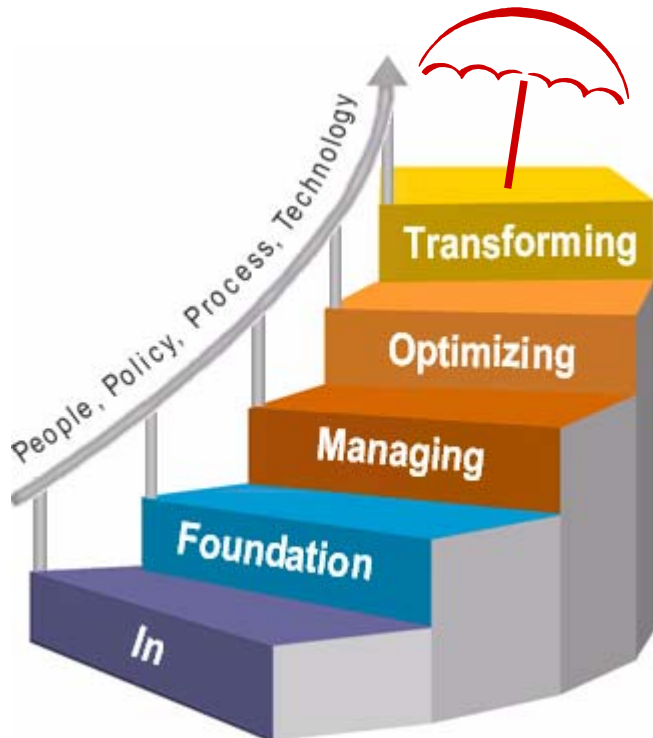
## Risk Qualification



**InfoSec CONTROLS must be based on Risk Prioritization**

# InfoSec Control Maturity

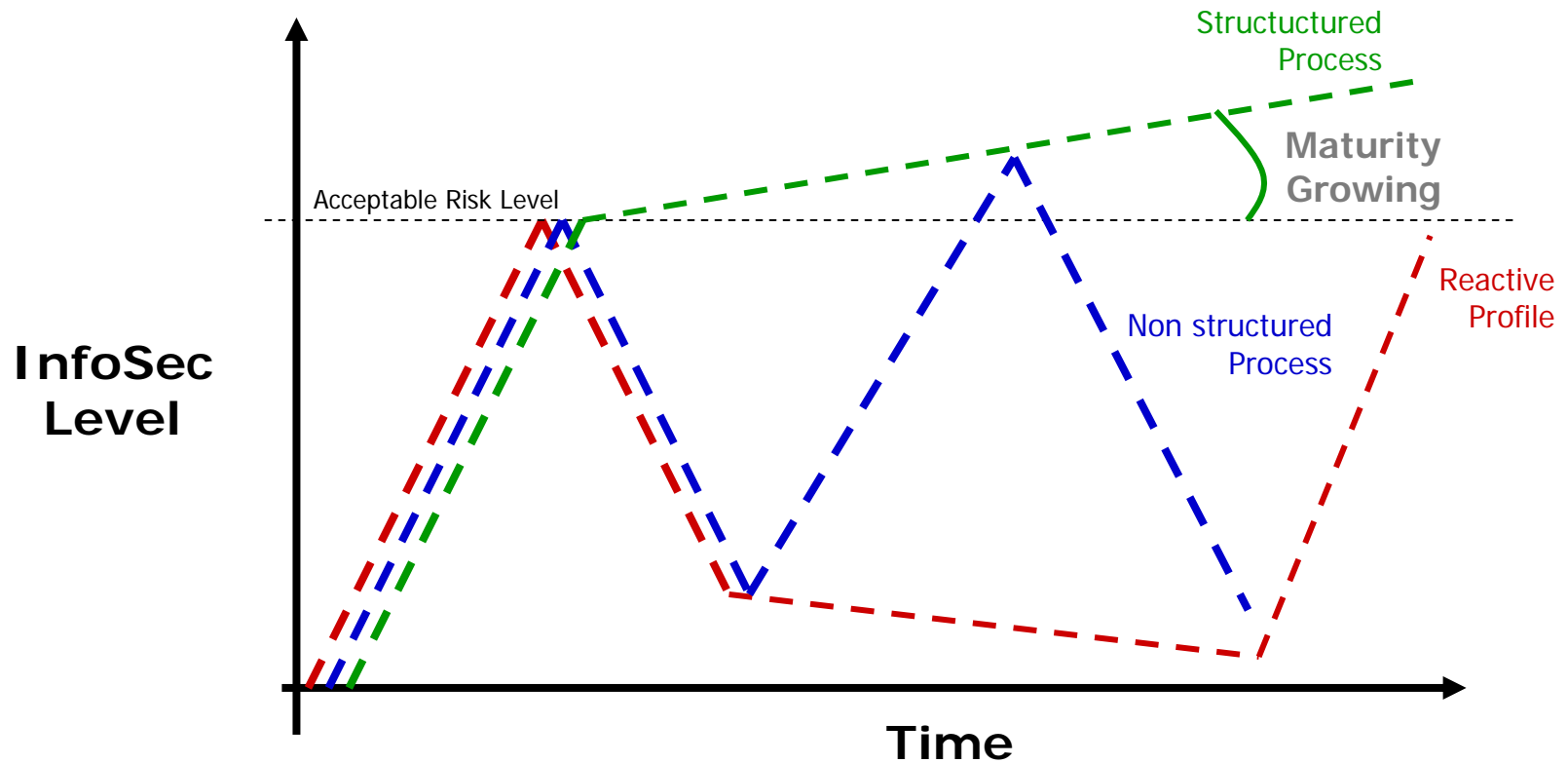
## Maturity Model



<b>0</b>	<b>Non-existent</b> Management processes are not applied at all
<b>1</b>	<b>Initial</b> Processes are ad hoc and disorganized
<b>2</b>	<b>Repeatable</b> Processes follow a regular pattern
<b>3</b>	<b>Defined</b> Processes are documented and communicated
<b>4</b>	<b>Managed</b> Processes are monitored and measured
<b>5</b>	<b>Optimized</b> Best practices are followed and automated

# InfoSec Maturity Growing

## Profiles of Risk Management



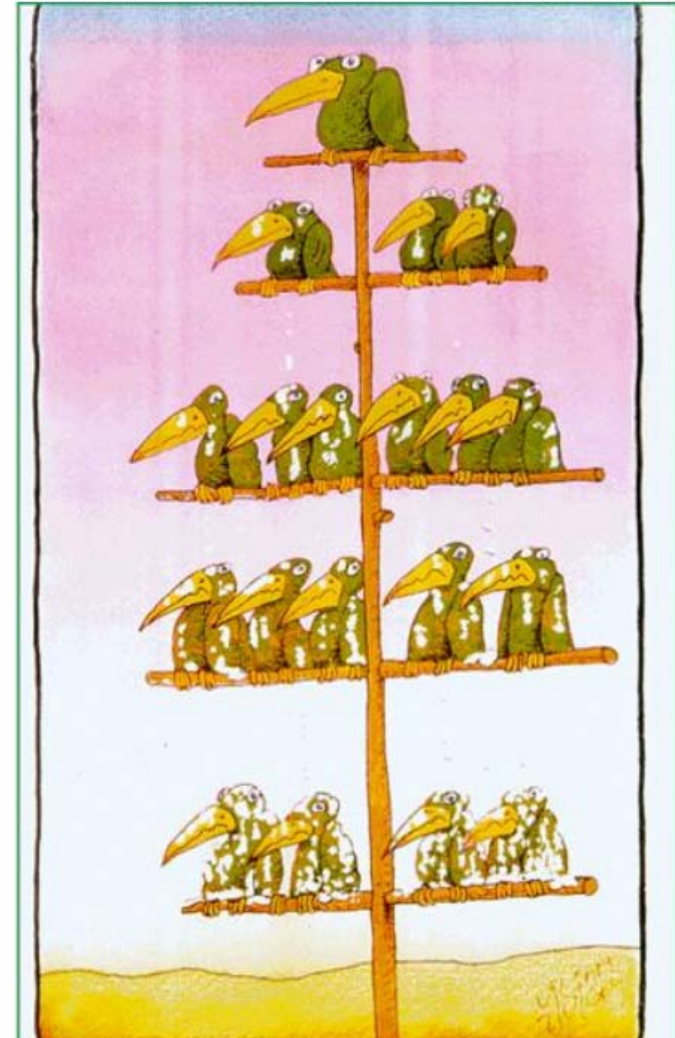
# Info Risk Governance Concept

## Key Message

**What you can't control  
you can't **MEASURE**.**

**What you can't  
measure you can't  
**MANAGE**.**

**What you can't manage  
you can't **IMPROVE**.**





# Manage Info Risk is...



**Know all info risk relevant aspects  
(people, tech and process)**



**Evaluate risk situations to prioritize  
and balance countermeasures**



**Maintain and be aligned with  
an integrated vision of risk management**



**Forecast potential scenarios of risk to  
dimension proactive investments**



**Trust that behavior is an important  
source of risk and also solutions**



**Be ready to manage crisis situations to  
mitigate business impacts**  
[www.semola.com.br](http://www.semola.com.br)

**Thank you.**

**Marcos Sêmola, CISM**  
marcos@semola.com.br