

# Security Metrics

Peter Versmissen

September 20<sup>th</sup> 2007

# Agenda

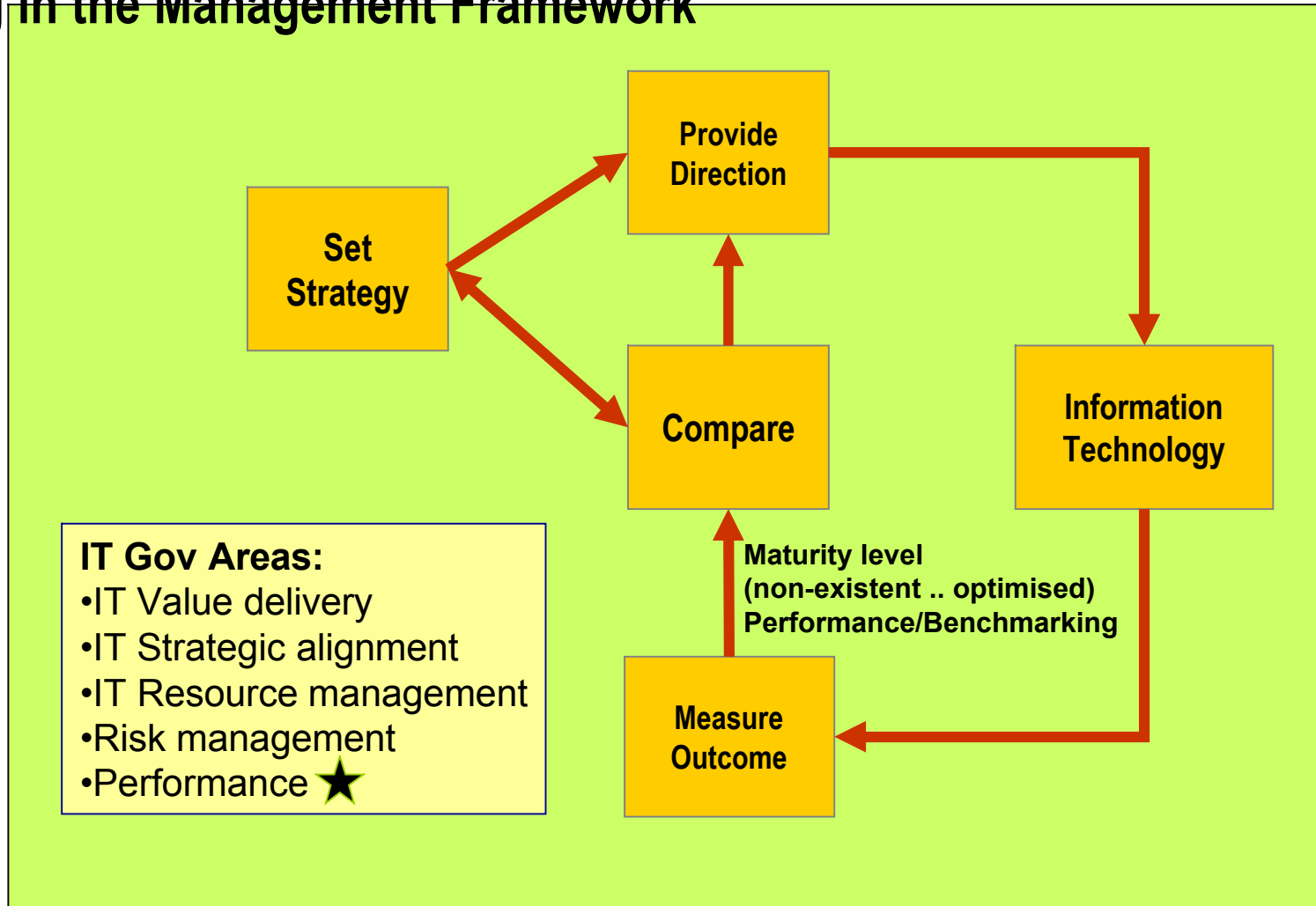
Security metrics – what and why

Security metrics – how

Case study

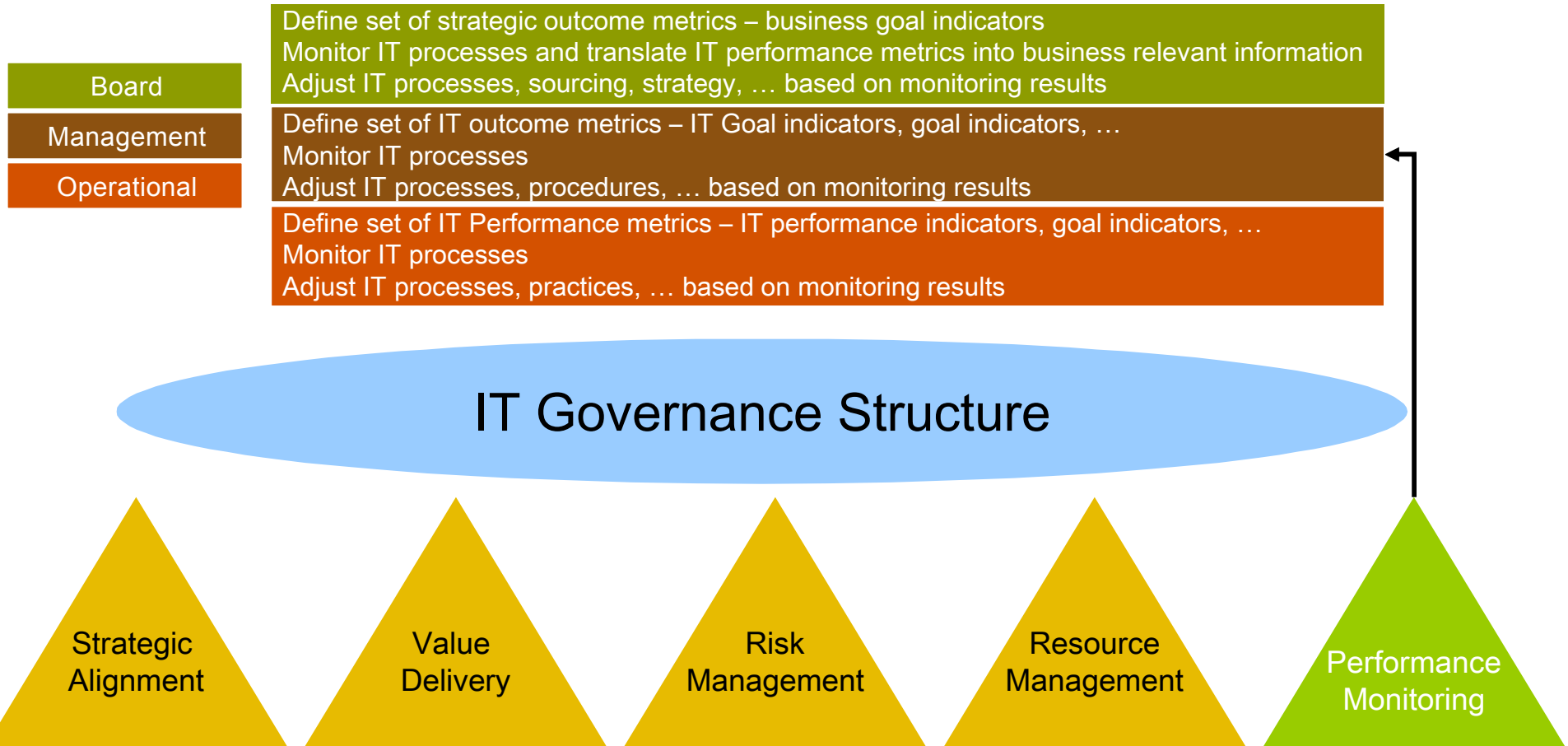
# Security metrics – what and why

## Situating in the Management Framework



# Security metrics – what and why

## Situating in the IT Gov Framework



# Security metrics – what and why

## Definition

- “security metrics should be objective, quantifiable measures against specific targets that enable an organisation to judge the effectiveness of information security in that organisation”

## Reasons for using security metrics

Typical reasons for using security metrics include:

- showing the **effectiveness and efficiency** of information security,
- indicating **compliance** to legislation and regulation, and
- demonstrating the **value** of information security

# Agenda

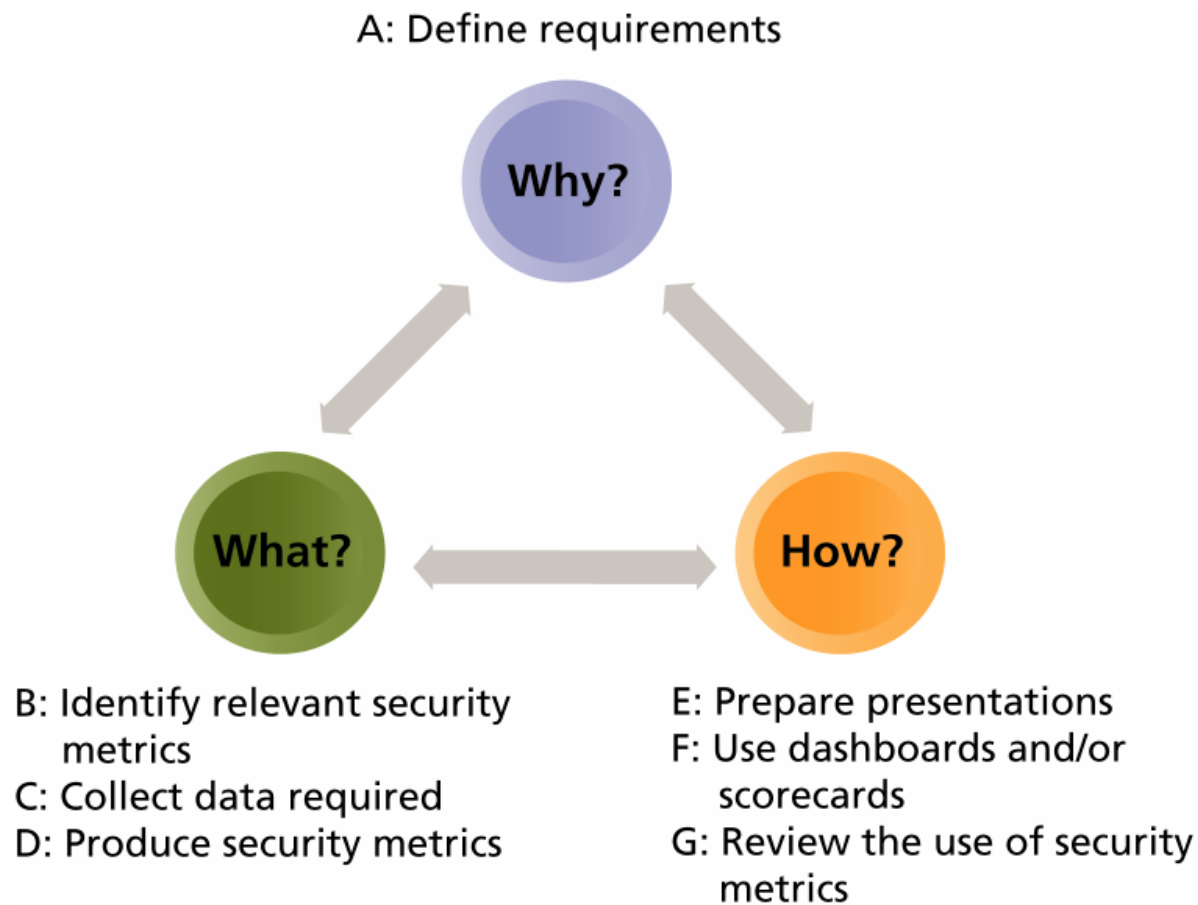
Security metrics – what and why

Security metrics – how

Case study

# Security metrics – how

## Producing security metrics



# Security metrics – how

## Characteristics

### Sample characteristics include:

- **Purpose:** What the security metric is designed to do
- **Cost:** An estimate or actual cost of collecting the security data
- **Type:** What the security metric is, for example: technical or managerial; leading or lagging; numerical or textual
- **Location:** Where the data for the security metric can be collected
- **Frequency:** How often the data needs to be collected / the security metric needs to be presented
- **Category:** E.g. number, frequency, duration, cost, ...);
- **Start/stop criteria:** for starting and stopping the collection of data for the security metric use and presentation of the security metric;
- **Duration of collection:** An estimate of, or actual, time period in which data will be collected

# Security metrics – how

## Examples

- The most common security metrics in use today are related to:
  - incidents
  - virus protection
  - risk management
  - cost
  - patch management
  - compliance
  - audit

# Agenda

Security metrics – what and why

Security metrics – how

Case study

# Case study

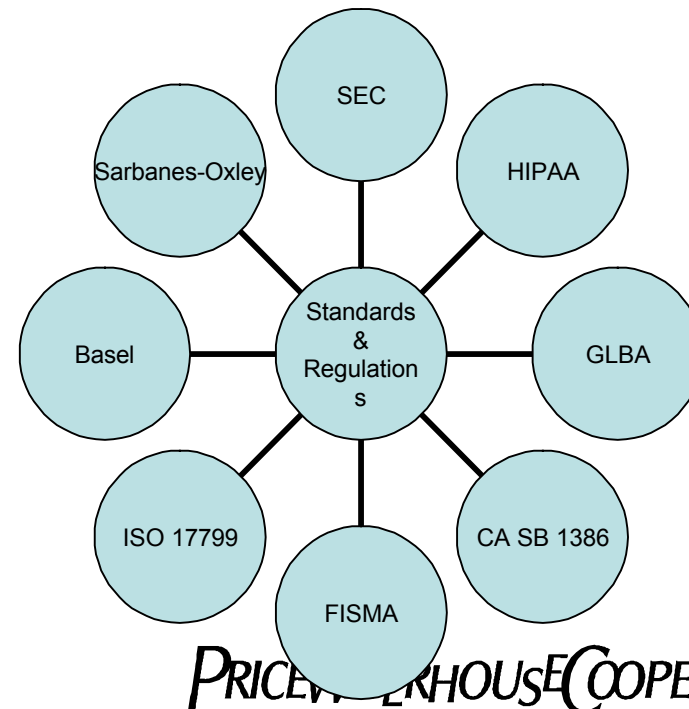
## Security dashboard case rationale

- Client in Energy industry, study executed in 2006 – highlights:
  - Increasing **corporate governance and privacy regulations** make information security problems an important challenge for businesses today
  - The aim of a security dashboard is to provide executives with the information they need to accurately **assess the companies' security status**.
  - The information of a security dashboard can **drive changes** that will help improve business performance
  - It is also a way to get more **senior management level support** by presenting them the IT Security status in a language they understand, creating a bridge between IT professionals and the business executives
  - Has its roots in the **balanced scorecard** from Kaplan & Norton to assess a company's performance on multiple dimensions

# Case study

## Security dashboard features

- Ability to present and summarize information in an **easy-to-understand graphic**
- **Drill-down capabilities** to get to detailed information and trend analysis behind the aggregated numbers and graphics
- The option to make **reports** which can be used to send the information to the appropriate parties
- **Support** for the current information security standards and regulations (ISO 17799, Sarbanes-Oxley, etc.)



# Case study

## Security dashboard approach – definition phase

The PwC approach for this assignment was made up of 6 key steps:

1. Agree on goal & objectives of Security Dashboard
2. Define metrics to be generated
3. Identify sources of information
4. Based on identified audience → agree on reporting types
5. Assess: buy vs. build
6. Implement solution

# Case study

## Security dashboard approach: realisation phase

The actual realisation could be broken down in two workstreams:

1

**Screening of the market regarding Security Dashboard software**

- match between the needs of Client and the proposed solution
- based on PwC experience and vendor knowledge

2

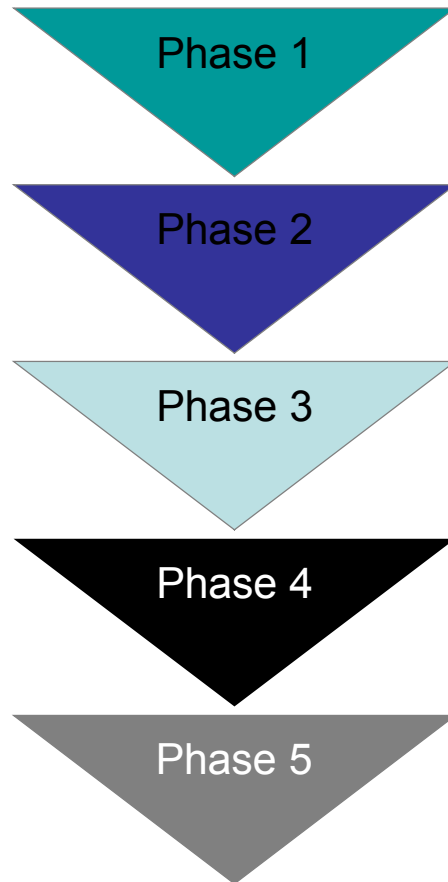
**Construction of an Excel-based Security Dashboard**

- based on ISO 17799:2005 (de facto information security standard)
- data feeds from the various Client IT systems
- in accordance with PwC best practices

# Case study

## Approach for market analysis

1



Requirements gathering of Client through interviews with the Security Officer
Matching and adding of requirements with PwC experience and best practices
Screening of the market using PwC databases and vendor information
Conducting vendor meetings, web conferences and interviews
Short list with possible vendors

# Case study

1

## Findings of market analysis

There are 3 different types of software solutions on the market that support security dashboard reporting:

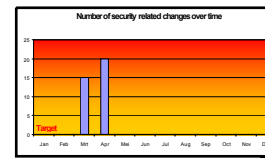
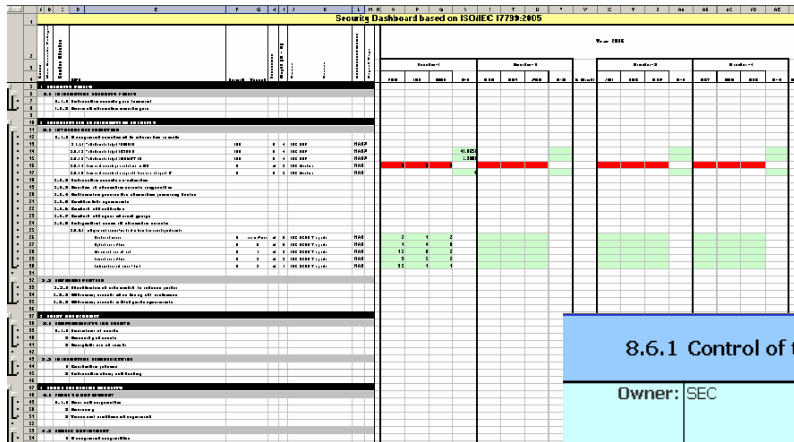
Type	Vendors
1. Security Dashboards which are part of a more sophisticated (network) security management system	Ubizen/Cybertrust, Skybox, netForensics, RSA Compliance Manager
2. Security Dashboard solutions who generate reports based on the data gathered by company-wide questionnaires (ad-hoc view on situation)	RiskWatch, Infosecure
3. Security Dashboard solutions which automatically or manually fetch data from the different IT systems of the organisation and report them	Dynasec, Host Analytics, Intellitactics, RippleTech

# Case study

2

## Excel version now implemented

- Interviews with different IT professionals were executed
- PwC developed the ISO 17799:2005-based dashboard with the maximum amount of automated controls
- Graphics, weights and targets for certain Key Performance Indicators are set up according to the PricewaterhouseCoopers best practices and will be aligned with specific client requirements.



8.6.1 Control of technical vulnerabilities		Year 2006	Prepared by: SBO
			As of: March
			Next Update: April
Owner:	SEC	Objective:	The target is to have 100% of the PC's and Servers with up to date patches
Measure:	# of events	Data Source:	These figures are not measurable yet

# Case study

## Conclusion of case study

- Security Dashboards are still an emerging subject within IT security, driven by the increasing need for corporate governance.
- The dashboard metrics should be tailored to the specific situation.

## Overall Conclusion

- Although all desired features have not yet be completed addressed, we propose to deploy the Excel version as alternative solution for the time being
- Additionally, Client should monitor the evolution of Security Dashboard market closely and re-evaluate its maturity (i.e. based on pricing, integrated solution with other technologies, ease-of-customisation, etc.) over the next 12 months



# Thank you