Using Software Measurement to Ensure Compliance

Martin Tennant

Compass Management Consulting Group

Introduction

- With software development and support becoming more complex, the need to ensure appropriate measurements exist is more important than ever before…
  - …its not just that a sound measurement framework should yield improvements in productivity and reductions in unit cost…
  - …its not even that the greater use of third parties demands sound governance structures with objective fact-based measures of performance…
  - …its mainly the fact that if you don't measure what's happening in your development and support portfolios these days then you, your boss and your boss's boss could be facing daunting compliance issues

Introduction

- *"The mistake many organizations make is to look at compliance as a one-time task when, in reality, it is an ongoing process that requires constant monitoring and updating"*

- *"Compliance is killing us, 48% of my development budget is being spent on SOX, Basel and a host of other regulations."*

The Compliance Framework

- Across the globe, legislative Corporate governance frameworks have been established
- The most well known is the Sarbanes-Oxley (SOX) code in the States
- But most European countries have established their own codes:
  - Lippens – Belgium
  - Tabaksblat – The Netherlands
  - Principes de gouvernement d'enterprise – France
  - Combined Code on Corporate Governance - UK

The Compliance Headache

- Why should IT be interested in this? After all isn't this a problem for the CEO and the CFO?
  - IT runs the applications that ensure financial compliance…
  - …so IT spends a great deal of money to ensure that legacy applications are in line with the legislation…
  - … and IT invests a great deal of the capital of the business in new product development

- Rest assured, the CEO and/or the CFO will have made it your problem…

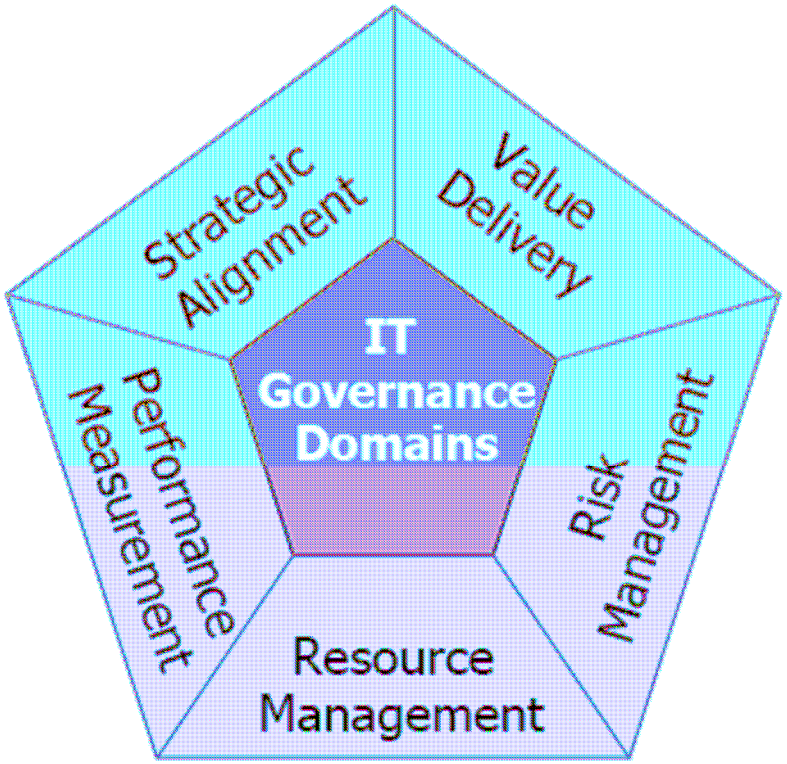
Implications

- Anything you disclose to the public is affected
  - Start with you annual report and work backwards from there!
  - You'll soon build up a substantial list of analyst reports, trading statements, contractual statements, bid statements…
- …and that impacts on all your internal financial controls!
  - In the business and in IT

The Compliance Solutions

- Use a standard framework for IT (CobiT)
  - Control objectives identify the things with which IT should comply
- Put the CIO on the Audit Committee
  - (and the Audit Committee needs to sit on IT)
- Use process controls within AD and AM (CMM and ITIL respectively)
- Introduce metrics for compliance into your business processes and your IT processes

CobiT – Some example metrics for Value Delivery



- How many IT related business projects do you currently have?
- What is the total cumulative budget?
- What proportion of your projects are mandatory or discretionary?
- What is the expected ROI on your key discretionary projects?
- What is your solutions delivery performance history? How will this affect your future ROI?
- How many projects were cancelled last year? What were the reasons?
- What is your CMM level for systems development/implementation processes?
- To what extent do executive bonuses depend upon satisfactory project delivery?
- Do you have reliable metrics to determine whether business case returns have actually been achieved?

The Role of Software Measurement

- In the software development life cycle there needs to be:
  - Factual, *auditable* metrics on the investments made by the organisation
  - Clear lines of responsibility and escalation
  - Evidence of periodic review of the investments, including plans to actuals and earned value
  - A greater focus will also be placed on testing for compliance and risk avoidance

- All the above needs to be incorporated into your development life cycle

The Role of Software Measurement

- In the production environment there need to be
  - A comprehensive service catalogue
  - Clear business-related metrics for availability, accuracy and so on
  - Audit trails for all software changes applied

- All the above needs to be incorporated into your development life cycle – maybe through the adoption of ITIL

Conclusion

- Audit is everywhere!
- Compliance isn't just a Board problem – it applies to all parts of the business
- IT needs to be part of the compliance solution…
- … and being able to demonstrate compliance means having the auditable facts to hand
- Software measurement is a therefore a vital tool in ensuring compliance