COBIT Framework for IT Governance and Control

José António Oliveira

Novembro/2011

Agenda

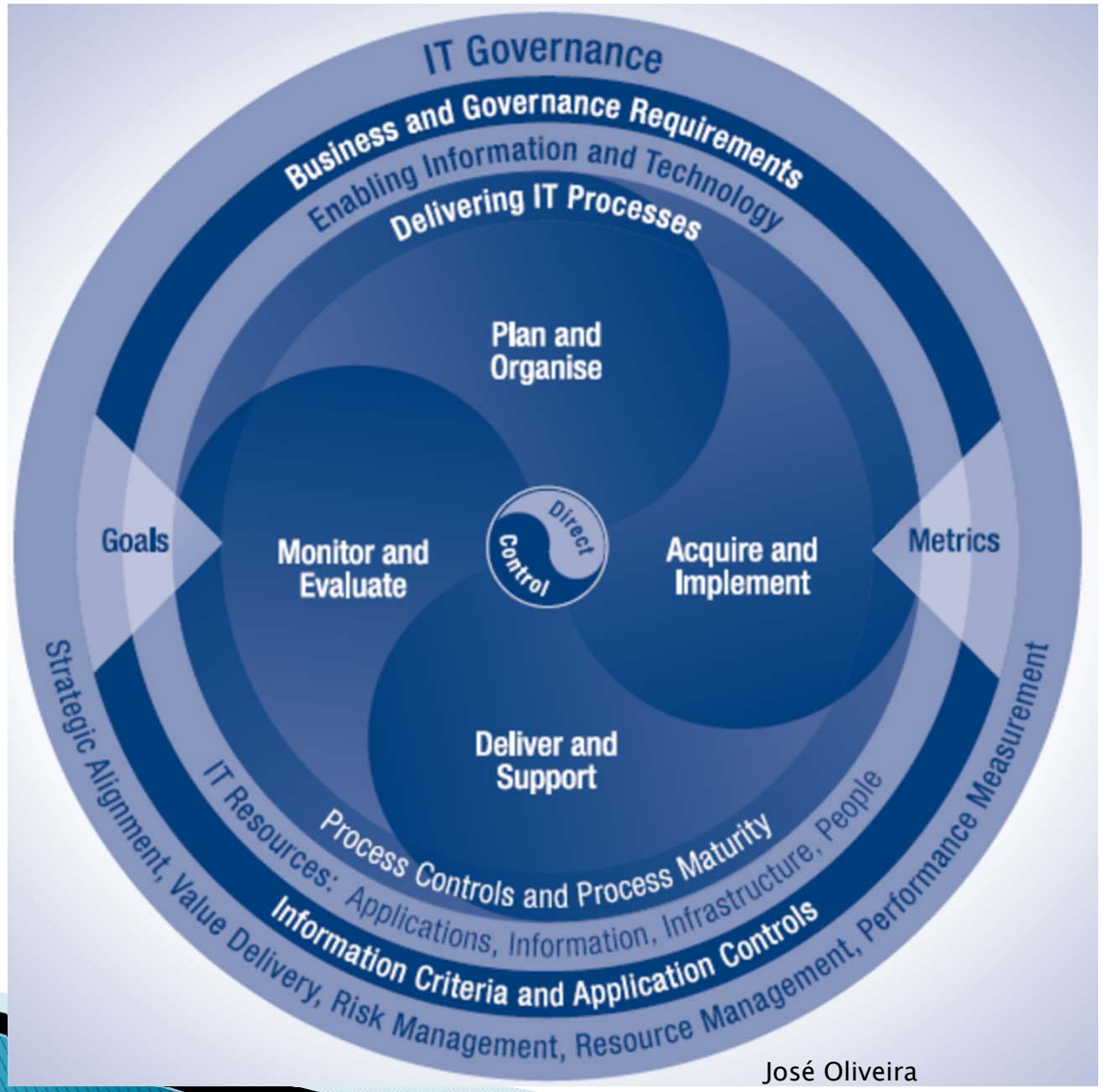
- Framework COBIT
- Visão do COBIT
- Aplicação do COBIT
  - Governação das TI
  - Aplicação em auditoria
- Exemplos de aplicação em auditoria
  - Avaliação da continuidade do negócio
  - Caracterização da despesa em TIC na administração pública (estratégia, riscos e mercados)

Framework COBIT

- Modelo orientado para a governação das tecnologias de informação

- *Framework* internacional unificadora que integra os principais standards de TI, incluindo ITIL, CMMI e ISO 17799.

Framework COBIT



COBIT Versão 4.1

Visão do COBIT

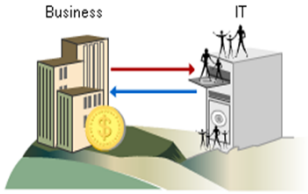
- O negócio determina as necessidades de informação e estas determinam as necessidades de tecnologia

- A sobrevivência das organizações depende da gestão efetiva da informação e da tecnologia associada:
  - Aumento da dependência dos SI
  - Aumento das vulnerabilidades e ameaças
  - Escala de custos com os SI
  - Potencial das TI

Aplicação do COBIT

- 2 vertentes:
  - Governação de TI – Implementação da *Framework* para:
    - Garantir que as TI têm um nível de governação adequado
    - Responder a exigências legais (ex. Sarbanes-Oxley)
    - Satisfazer métricas exigidas internacionalmente
    - …
  - Auditoria – Utilização da *Framework* para:
    - Definir o âmbito do trabalho
    - Comparar os resultados obtidos com os níveis considerados como adequados
    - Usar uma métrica standard (reconhecida)
    - Agregar resultados obtidos em auditorias efetuadas a diferentes entidades ou em ambientes heterogéneos
    - …

Desafios da Governação das TI

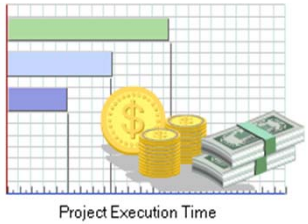


Alinhar TI com o negócio

Segurança

Manter TI a funcionar

Gerir a Complexidade



Valor/Custos

Conformidade Legal

- As organizações precisam de:
  - Uma abordagem estruturada para gerir estes desafios
  - Assegurar objetivos negociados para as TI, controlos de gestão adequados e monitorização eficaz de performance para funcionar sem surpresas

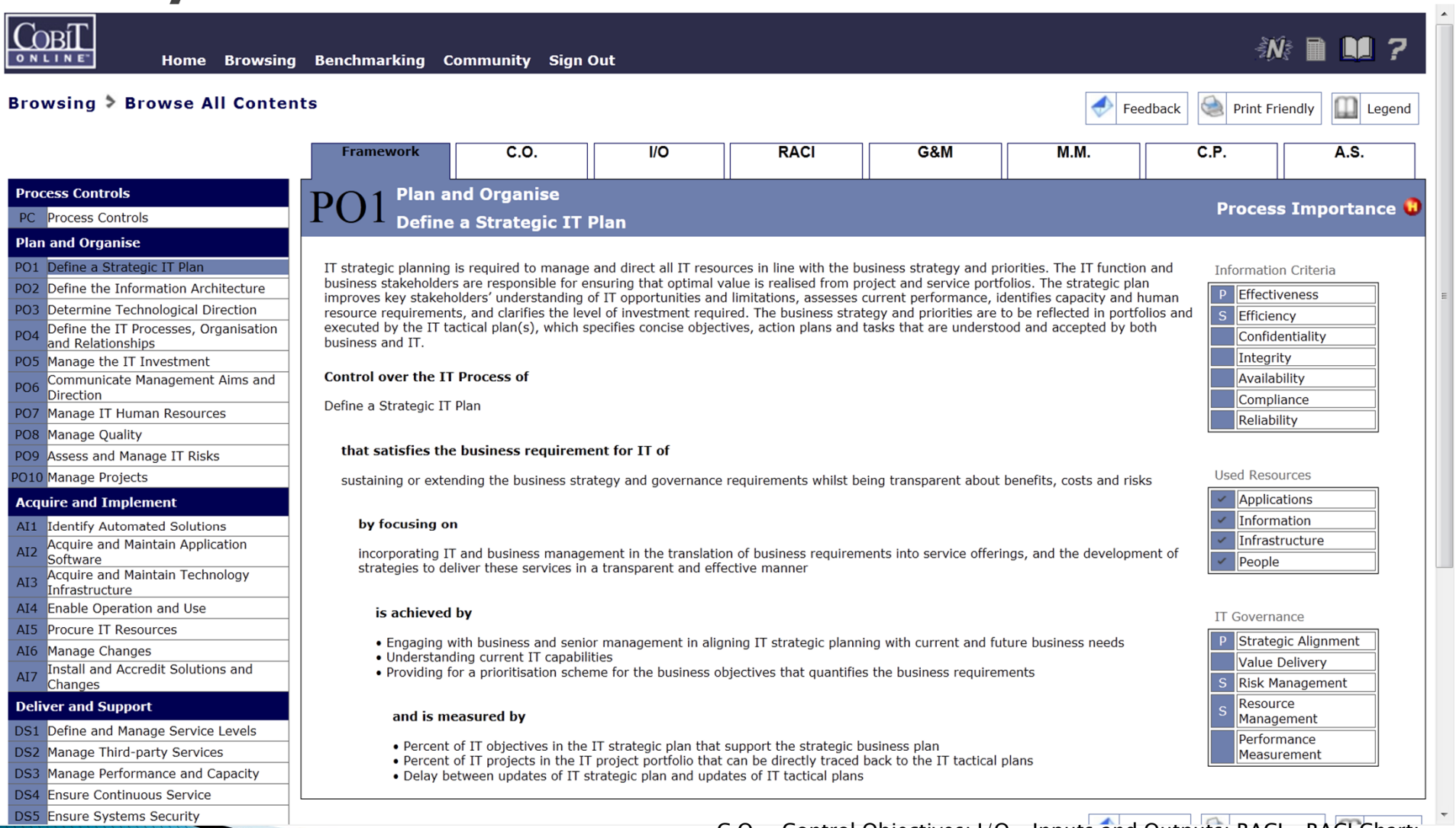
COBIT – Auditoria TIC na IGF

- Definição do trabalho a realizar
- Definição dos objetivos da auditoria
- Delimitação do âmbito
- Estudo inicial da entidade ou setor de atividade a auditar
  - Seleção das entidades

COBIT – Auditoria TIC na IGF

- Seleção do(s) domínio(s) do COBIT:
  - Determinar os processos e respetivos objetivos de controlo a avaliar:
    - Estão sujeitos aos objetivos do trabalho, ao âmbito definido, bem como, aos resultados do estudo inicial
  - Seleção da métrica a utilizar:
    - CMMI (*Capability Maturity Model Integration*); e/ou
    - Níveis de risco (Alto/Médio/Baixo)
  - Determinar os níveis adequados ou recomendados dos processos (quando possível)

MyCOBIT On-line



C.O. – Control Objectives; I/O – Inputs and Outputs; RACI – RACI Chart; G&M – Goals and Metrics; M.M. – Maturity Models; C.P. – Control Practices; A.S. – Assurance Steps

COBIT – Auditoria TIC na IGF

- Elaboração do plano de auditoria
  - Atividades
  - Recursos
  - Tempos

COBIT – Auditoria TIC na IGF

- Trabalho de campo
  - Utilização frequente de questionários e programas de auditoria
  - Para que se adapte as exigências dos processos do COBIT à própria entidade é fundamental tomar em consideração (entre outros aspetos):
    - O ambiente concreto em que está envolvida a entidade e
    - O core business

      - Exemplo: Os níveis de exigência em governação de TI para um Instituto de Informática ou uma DGCI não poderão ser idênticos aos níveis de exigência de uma DGAL
        - Os primeiros têm de manter altos níveis de performance
        - Para o outro os níveis poderão ser os mínimos que garantam a integridade, disponibilidade e confidencialidade dos sistemas e da informação

COBIT – Auditoria TIC na IGF

- Relatório
  - Elaboração de um relatório (sujeito a contraditório) por entidade
    - As conclusões são específicas por entidade
    - As recomendações são de caracter estratégico, tático e operacional, mas sempre focadas na entidade
    - Ambas (conclusões e recomendações) têm em consideração apenas a avaliação específica da entidade
      - Por exemplo: Não se recomenda a implementação de um controlo caro, previsto pelo COBIT, para proteger um "bem" (*asset*) cujo valor é baixo

COBIT – Auditoria TIC na IGF

- Relatório
  - Elaboração de um relatório global do setor de atividade (não sujeito a contraditório)
    - As conclusões são gerais do setor de atividade (ex: Ministério)
    - As recomendações são de caracter político, estratégico e legislativo
    - Não têm em consideração situações específicas de entidades
    - Tem em consideração os níveis considerados como adequados pelo COBIT

Exemplo de aplicação

- Avaliação da continuidade do negócio
  - Domínios do COBIT
    - DS – Deliver and Support
  - Processos avaliados
    - DS4 – Garantia de Continuidade do Serviço
  - Objetivos de Controlo
    - Estratégia e Filosofia do Plano de Continuidade de TI
    - Conteúdo do Plano de Continuidade de TI
    - Minimização dos requisitos de continuidade de TIs
    - Manter no Plano de Continuidade de TI
    - Teste do Plano de Continuidade
    - Formação sobre o Plano de continuidade de TI
    - Distribuição do Plano de Continuidade de TI
    - Recursos de TI Críticos
    - Local e Hardware de Backup
    - Armazenamento de Backups
    - Procedimentos de Wrap-up

Resultados

Entidade \ Nível de Risco	Continuidade de serviço	Dependência face ao *Outsourcing*	*Backup* e recuperação
[redacted]	Alto	Médio	Baixo
[redacted]	Médio	Baixo	Baixo
[redacted]	Médio	Baixo	Baixo
[redacted]	Médio	Médio	Médio
[redacted]	Alto	Médio	Baixo
[redacted]	Alto	Baixo	Baixo
[redacted]	Alto	Alto	Baixo
[redacted]	Médio	Baixo	Baixo

Exemplo de aplicação

- Caracterização da despesa em TIC na administração pública (estratégia, riscos e mercados)
  - Domínios do COBIT
    - PLANEAMENTO E ORGANIZAÇÃO (PO)
  - Processos avaliados
    - PO1 – "DEFINIR UM PLANO ESTRATÉGICO DE TI"
    - PO2 – "DEFINIR A ARQUITECTURA DA INFORMAÇÃO"
    - PO3 – "DETERMINAR A DIRECÇÃO TECNOLÓGICA"
    - PO4 – "DEFINIR OS PROCESSOS DE TI, ORGANIZAÇÃO E RELACIONAMENTOS"
    - PO5 – "GERIR O INVESTIMENTO EM TI"
    - PO6 – "COMUNICAR AS METAS E AS LINHAS DE ORIENTAÇÃO DE GESTÃO"
    - PO7 – "GERIR OS RECURSOS HUMANOS DE TI"
    - PO8 – "GERIR A QUALIDADE"
    - PO9 – "AVALIAR E GERIR OS RISCOS DE TI"
    - PO10 – "GESTÃO DE PROJECTOS"

Resultados

Nível de risco associado à Maturidade dos processos de Planeamento e Organização em TIC na Administração Pública

Relevância dos processos em Planeamento e Organização (ISACA)	Alta	Média	Baixa
Alto	PO9	PO1; PO10	
Médio	PO8	PO3; PO5; PO6	
Baixo		PO2; PO4; PO7	

Legenda:

Relevância dos Processos COBIT	
Processos	**Relevância**
PO1 - Definir um Plano Estratégico de TI	Alta
PO2 - Definir a Arquitectura de Informação	Baixa
PO3 - Determinar a Direcção Tecnológica	Média
PO4 - Definir os Processos de TI, Organização e Relacionamento	Baixa
PO5 - Gerir o Investimento em TI	Média
PO6 - Comunicar as Metas e as Orientações de Gestão	Média
PO7 - Gerir Recursos Humanos de TI	Baixa
PO8 - Gerir a Qualidade	Média
PO9 - Avaliar e Gerir Riscos de TI	Alta
PO10 - Gestão de Projectos	Alta

Nível de Risco Associado à Maturidade	
Nível de Maturidade	**Risco Associado**
0 – Inexistente	Alto
1 – Inicial / *Ad Hoc*	
2 – Repetitivo mas intuitivo	Médio
3 – Definido	
4– Gerido e Mensurável	Baixo
5 – Optimizado	

Conclusões

- O COBIT pode ser aplicado para:
  - Aplicar controlos adequados à governação das TIC
  - Facilitar o trabalho dos auditores (internos e externos)
  - Ser usado como programa de auditoria das TIC
  - As métricas (CMMI / níveis de risco) permitem:
    - Efetuar trabalhos comparáveis
    - Medir a performance da governação de TIC de um organismo ou setor de atividade
    - Comparar os resultados obtidos com os níveis standard internacionais

Questões

Referências

- COBIT – ISACA
  - www.isaca.org/cobit

Obrigado

Contacto:

José António Oliveira
joseoliveira@igf.min-financas.pt