

## COBIT

*Um kit de ferramentas para a excelência na gestão de TI*

Eduardo Mayer Fagundes  
*e-mail: eduardo@efagundes.com*

### **Introdução**

Atualmente, é impossível imaginar uma empresa sem uma forte área de sistemas de informações (TI), para manipular os dados operacionais e prover informações gerenciais aos executivos para tomadas de decisões. A criação e manutenção de uma infra-estrutura de TI, incluindo profissionais especializados requerem altos investimentos. Algumas vezes a alta direção da empresa coloca restrições aos investimentos de TI por duvidarem dos reais benefícios da tecnologia. Entretanto, a ausência de investimentos em TI pode ser o fator chave para o fracasso de um empreendimento em mercados cada vez mais competitivos. Por outro lado, alguns gestores de TI não possuem habilidade para demonstrar os riscos associados ao negócio sem os corretos investimentos em TI. Para melhorar o processo de análise de riscos e tomada de decisão é necessário um processo estruturado para gerenciar e controlar as iniciativas de TI nas empresas, para garantir o retorno de investimentos e adição de melhorias nos processos empresariais. Esse novo movimento é conhecido como Governança em TI, ou "*IT Governance*".

O termo "*IT governance*" é definido como uma estrutura de relações e processos que dirige e controla uma organização a fim de atingir seu objetivo de adicionar valor ao negócio através do gerenciamento balanceado do risco com o retorno do investimento de TI.

Para muitas organizações, a informação e a tecnologia que suportam o negócio representa o seu mais valioso recurso. Além disso, num ambiente de negócios altamente competitivo e dinâmico é requerido uma excelente habilidade gerencial, onde TI deve suportar as tomadas de decisão de forma rápida, constante e com custos cada vez mais baixos.

Não existem dúvidas sobre o benefício da tecnologia aplicada aos negócios. Entretanto, para serem bem sucedidas, as organizações devem compreender e controlar os riscos associados no uso das novas tecnologias. O CobiT (*Control Objectives for Information and related Technology*) é uma ferramenta eficiente para auxiliar o gerenciamento e controle das iniciativas de TI nas empresas.

### **O que o CobiT?**

O CobiT é um guia para a gestão de TI recomendado pelo ISACF (*Information Systems Audit and Control Foundation*, [www.isaca.org](http://www.isaca.org)). O CobiT inclui recursos tais como um sumário executivo, um *framework*, controle de objetivos, mapas de auditoria, um conjunto de ferramentas de implementação e um guia com técnicas de gerenciamento. As práticas de gestão do CobiT são recomendadas pelos peritos em gestão de TI que ajudam a otimizar os investimentos de TI e fornecem métricas para avaliação dos resultados. O CobiT independe das plataformas de TI adotadas nas empresas.

O CobiT é orientado ao negócio. Fornece informações detalhadas para gerenciar processos baseados em objetivos de negócios. O CobiT é projetado para auxiliar três audiências distintas:

- Gerentes que necessitam avaliar o risco e controlar os investimentos de TI em uma organização.
- Usuários que precisam ter garantias de que os serviços de TI que dependem os seus produtos e serviços para os clientes internos e externos estão sendo bem gerenciados.
- Auditores que podem se apoiar nas recomendações do CobiT para avaliar o nível da gestão de TI e aconselhar o controle interno da organização.

O CobiT está dividido em quatro domínios:

- Planejamento e organização.
- Aquisição e implementação.
- Entrega e suporte.
- Monitoração.

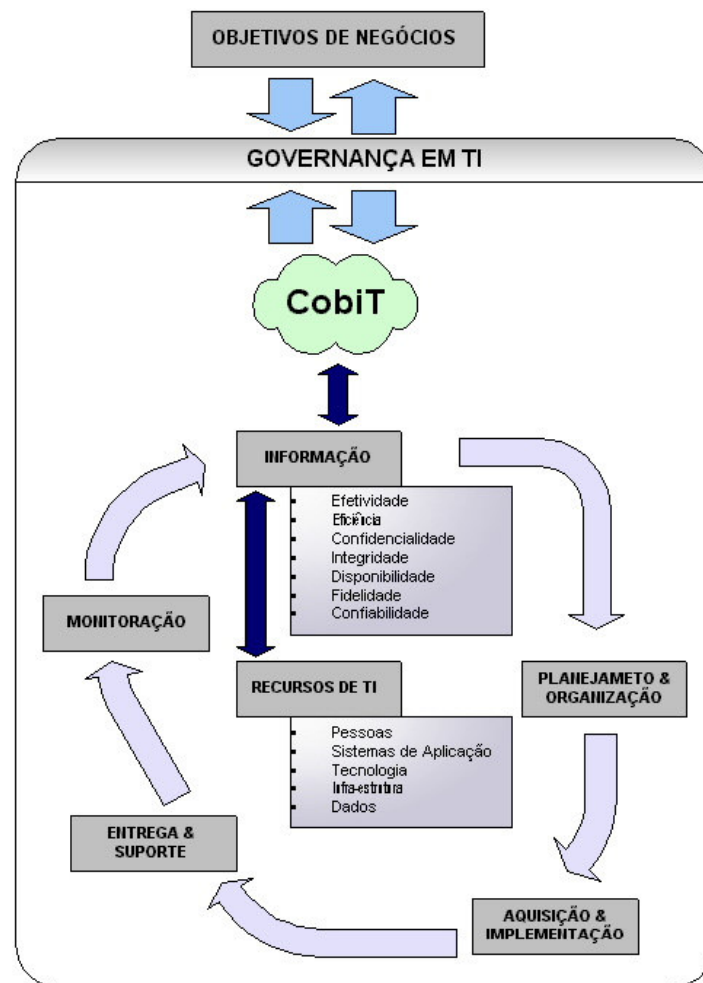


Figura 1: Os quatro domínios do CobiT

A figura 1 ilustra a estrutura do CobiT com os quatro domínios, onde claramente está ligado aos processos de negócio da organização. Os mapas de controle fornecidos pelo CobiT auxiliam os auditores e gerentes a manter controles suficientes para garantir o acompanhamento das iniciativas de TI e recomendar a implementação de novas práticas, se necessário. O ponto central é o gerenciamento da informação com os recursos de TI para garantir o negócio da organização.

Cada domínio cobre um conjunto de processos para garantir a completa gestão de TI, somando 34 processos:

*Planejamento e Organização*

- Define o plano estratégico de TI
- Define a arquitetura da informação
- Determina a direção tecnológica
- Define a organização de TI e seus relacionamentos
- Gerencia os investimento de TI
- Gerencia a comunicação das direções de TI
- Gerencia os recursos humanos
- Assegura o alinhamento de TI com os requerimentos externos
- Avalia os riscos
- Gerencia os projetos
- Gerencia a qualidade

*Aquisição e implementação*

- Identifica as soluções de automação
- Adquire e mantém os softwares
- Adquire e mantém a infra-estrutura tecnológica
- Desenvolve e mantém os procedimentos
- Instala e certifica softwares
- Gerencia as mudanças

*Entrega e suporte*

- Define e mantém os acordos de níveis de serviços (SLA)
- Gerencia os serviços de terceiros
- Gerencia a performance e capacidade do ambiente
- Assegura a continuidade dos serviços
- Assegura a segurança dos serviços
- Identifica e aloca custos
- Treina os usuários
- Assiste e aconselha os usuários
- Gerencia a configuração
- Gerencia os problemas e incidentes
- Gerencia os dados
- Gerencia a infra-estrutura
- Gerencia as operações

### *Monitoração*

- Monitora os processos
- Analisa a adequação dos controles internos
- Prove auditorias independentes
- Prove segurança independente

## **Desenvolvimento do CobiT**

A primeira publicação foi em 1996 enfocando o controle e análise dos sistemas de informação. Sua segunda edição em 1998 ampliou a base de recursos adicionando o guia prático de implementação e execução. A edição atual, já coordenada pelo IT Governance Institute, introduz as recomendações de gerenciamento de ambientes de TI dentro do modelo de maturidade de governança.

O CobiT recebe um conjunto de contribuições de várias empresas e organismos internacionais, entre eles:

- Padrões técnicos da ISO, EDIFACT, etc.
- Os códigos de conduta emitidos pelo Conselho de Europa, OECD, ISACA, etc.
- Critérios de qualificação para TI e processos: ITSEC, TCSEC, ISO 9000, SPICE, TickIT, etc.
- Padrões profissionais para controle internos e auditoria: COSO, IFAC, AICPA, CICA, ISACA, IIA, PCIE, GAO, etc.
- Práticas e exigências dos fóruns da indústria (ESF, I4) e das plataformas recomendadas pelos governos (IBAG, NIST, DTI), etc.
- Exigências das indústrias emergentes como operação bancária, comércio eletrônico e engenharia de software.

## **Benefícios do CobiT**

Na era da dependência eletrônica dos negócios e da tecnologia, as organizações devem demonstrar controles crescentes em segurança. Cada organização deve compreender seu próprio desempenho e deve medir seu progresso. O *benchmarking* com outras organizações deve fazer parte da estratégia da empresa para conseguir a melhor competitividade em TI. As recomendações de gerenciamento do CobiT com orientação no modelo de maturidade em governança auxiliam os gerentes de TI no cumprimento de seus objetivos alinhados com os objetivos da organização.

Os *guidelines* de gerenciamento do CobiT focam na gerência por desempenho usando os princípios do *balanced scorecard*. Seus indicadores chaves identificam e medem os resultados dos processos, avaliando seu desempenho e alinhamento com os objetivos dos negócios da organização.

## **Ferramentas de Gerenciamento do CobiT**

Os modelos de maturidade de governança são usados para o controle dos processos de TI e fornecem um método eficiente para classificar o estágio da organização de TI. A governança de TI e seus processos com o objetivo de adicionar valor ao negócio através do

balanceamento do risco e retorno do investimento podem ser classificados da seguinte forma:

- 0 Inexistente
- 1 Inicial / Ad Hoc
- 2 Repetitivo mas intuitivo
- 3 Processos definidos
- 4 Processos gerenciáveis e medidos
- 5 Processo otimizados

Essa abordagem é derivada do modelo de maturidade para desenvolvimento de software, *Capability Maturity Model for Software (SW-CMM)*, proposto pelo *Software Engineering Institute (SEI)*. A partir desses níveis, foi desenvolvido para cada um dos 34 processos do CobiT um roteiro:

- Onde a organização está hoje
- O atual estágio de desenvolvimento da indústria (*best-in-class*)
- O atual estágio dos padrões internacionais
- Aonde a organização quer chegar

Os fatores críticos de sucesso definem os desafios mais importantes ou ações de gerenciamento que devem ser adotadas para colocar sobre controle a gestão de TI. São definidas as ações mais importantes do ponto de vista do que fazer a nível estratégico, técnico, organizacional e de processo.

Os indicadores de objetivos definem como serão mensurados os progressos das ações para atingir os objetivos da organização, usualmente expressos nos seguintes termos:

- Disponibilidade das informações necessárias para suportar as necessidades de negócios
- Riscos de falta de integridade e confidencialidade das informações
- Eficiência nos custos dos processos e operações
- Confirmação de confiabilidade, efetividade e conformidade das informações.

Indicadores de desempenho definem medidas para determinar como os processos de TI estão sendo executados e se eles permitem atingir os objetivos planejados; são os indicadores que definem se os objetivos serão atingidos ou não; são os indicadores que avaliam as boas práticas e habilidades de TI.

### **Mais informações**

Muitas informações do CobiT são padrões abertos e disponíveis gratuitamente para download no site do *IT Governance Institute's* [www.itgovernance.org](http://www.itgovernance.org) ou no site do *Information System Audit & Control Association* [www.isaca.org](http://www.isaca.org).

## DADOS DO AUTOR



Eduardo Mayer Fagundes estuda os impactos da tecnologia da informação e modelos de gestão de TI nas organizações, focando em tecnologia, técnicas e gestão de pessoas. Seu livro "Como Ingressar nos Negócios Digitais" foi publicado em parceria com o SEBRAE Nacional com o objetivo de ampliar a visão empresarial no comércio eletrônico.

Eduardo é graduado em engenharia elétrica, possui especialização em telecomunicações e é mestre em ciência da computação. Foi professor por mais de 20 anos em conceituadas instituições de ensino. Palestrante em vários seminários e congressos. Foi gerente de infra-estrutura e sistemas da Ford Brasil, responsável pelo desenho da infra-estrutura de TI da moderna fábrica da montadora em Camaçari-Bahia.

Atualmente é diretor de TI (CIO) das empresas do grupo americano AES no Brasil. A AES atua nos mercados de geração e distribuição de energia e na área de telecomunicações. A AES Eletropaulo, maior distribuidora de energia da América do Sul, é uma das empresas do grupo.

Escreve artigos no site [www.efagundes.com](http://www.efagundes.com).