

COBIT

Um kit de ferramentas para a excelência de TI

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 infraestrutura 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 é o CobiT?

O CobiT é um guia para a gestão de TI recomendado pelo ISACF (*Information Systems Audit and Control Foundation*, 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:

1. Planejamento e organização.
2. Aquisição e implementação.
3. Entrega e suporte.
4. Monitoração.

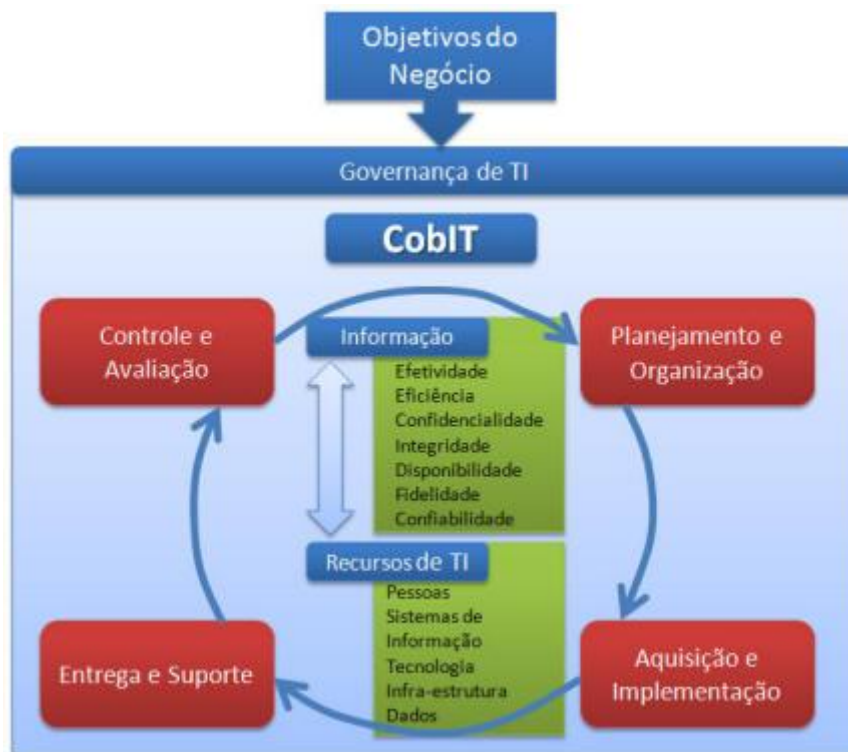


Figura 1: Os quatro domínios do CobIT

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

1. Define o plano estratégico de TI
2. Define a arquitetura da informação
3. Determina a direção tecnológica
4. Define a organização de TI, os seus processos e seus relacionamentos
5. Gerencia os investimentos de TI
6. Comunica os objetivos e direcionamentos gerenciais
7. Gerencia os recursos humanos
8. Gerenciar a qualidade

9. Avalia e gerencia os riscos de TI
10. Gerencia os projetos

Aquisição e implementação

1. Identifica as soluções de automação
2. Adquire e mantém os softwares
3. Adquire e mantém a infraestrutura tecnológica
4. Viabiliza a operação e utilização
5. Adquire recursos de TI
6. Gerencia as mudanças
7. Instala e aprova soluções e mudanças

Entrega e suporte

1. Define e mantém os acordos de níveis de serviços (SLA)
2. Gerencia os serviços de terceiros
3. Gerencia a performance e capacidade do ambiente
4. Assegura a continuidade dos serviços
5. Assegura a segurança dos serviços
6. Identifica e aloca custos
7. Educa e treina os usuários
8. Gerencia a central de serviços e incidentes
9. Gerencia a configuração
10. Gerencia os problemas
11. Gerencia os dados
12. Gerencia a infraestrutura
13. Gerencia as operações

Monitoração

1. Monitora e avalia o desempenho da TI
2. Monitora e avalia os controles internos
3. Assegura a conformidade com requisitos externos
4. Prove governança para a TI

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 Integrated for Software* (SW-CMMI), 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
- Confirmação de confiabilidade, efetividade e conformidade das informações.
- Eficiência nos custos dos processos e operações

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.

Para avaliação do nível de maturidade utiliza-se o *CobiT® Assessment Process*(CAP). O processo avalia os seguintes aspectos: propósito do processo; resultados do processo; descrição das práticas recomendadas para o processo (BP – *Base Practice*); entregáveis do processo (WP – *Work Product*); e, os processos dependentes ou requeridos para processo.

Para todas as BPs associadas ao processo avalia-se a capacidade para atender aos objetivos dos processos de negócio. A partir do resultado da avaliação é planejada ações para atingir o nível ideal de maturidade do processo.

Frameworks de Suporte

Os 34 processos do CobiT podem ser atendidos por outros modelos que definem boas práticas de gestão, tais como: ITIL, PMBOK, CMMI e ISO/IEC 27001 e 27002. Cada um desses modelos possui práticas definidas para a gestão de seus processos. A correta implantação dessas práticas garante que a entrega e qualidade dos produtos e serviços atendam as necessidades do negócio.

O ITIL (*IT Infrastructure Library*) é um dos modelos de gestão para serviços de TI mais adotados pelas organizações. O ITIL é um modelo não-proprietário e público que define as melhores práticas para o gerenciamento dos serviços de TI. Cada módulo de gestão do ITIL define uma biblioteca de práticas para melhorar a eficiência de TI, reduzindo os riscos e aumentando a qualidade dos serviços e o gerenciamento de sua infra-estrutura. O ITIL foi desenvolvido pela agência central de computação e telecomunicações do Reino Unido (CCTA) a partir do início dos anos 80.

O CMMI for software (*Capability Maturity Model Integrated for software*) é um processo desenvolvido pela SEI (*Software Engineering Institute, Pittsburg, Estados Unidos*) para ajudar as organizações de software a melhorar seus processos de desenvolvimento. O processo é dividido em cinco níveis sequenciais bem definidos: Inicial, Repetível, Definido, Gerenciável e

Otimizado. Esses cinco níveis provêm uma escala crescente para mensurar a maturidade das organizações de software. Esses níveis ajudam as organizações a definir prioridades nos esforços de melhoria dos processos.

O PMI (*Project Management Institute*) é a uma organização sem fins lucrativos de profissionais da área de gerenciamento de projetos. O PMI visa promover e ampliar o conhecimento existente sobre gerenciamento de projetos assim como melhorar o desempenho dos profissionais e organizações da área. As definições e processos do PMI estão publicados no PMBOK (*Guide to the Project Management Body of Knowledge*). Esse manual define e descrevem as habilidades, as ferramentas e as técnicas para o gerenciamento de um projeto. O gerenciamento de projetos compreende cinco processos – Início, Planejamento, Execução, Controle e Fechamento, bem com nove áreas de conhecimento: Integração, escopo, tempo, custo, qualidade, recursos humanos, comunicação, análise de risco e aquisição.

Para a gestão da segurança da informação são adotadas as normas da série ISO/IEC 27000, que contempla:

- ISO/IEC 27001, *Information Security Management Systems - Requirement*, definida para prover um modelo para estabelecer, implantar, operar, monitorar, rever, manter e melhorar um Sistema de Gestão da Segurança da Informação.
- ISO/IEC 27002, *Code of Practice for Information Security Management* (substitui a ISO 177799) que tem o objetivo de servir como um guia prático para desenvolver os procedimentos de segurança da informação e práticas eficientes de gestão da segurança para a organização.

Esses padrões devem ser adotados pelas organizações de TI em maior ou menor escala, dependendo da complexidade do negócio. Quanto mais complexo o negócio mais formal devem ser a implementação dos processos e seu controle. Se analisarmos as técnicas e as práticas recomendadas por esses padrões chegaremos a conclusão que são óbvias para uma boa gestão de TI, entretanto se as ignorarmos colocaremos em risco a empresa.

A adoção de padrões requer um controle efetivo que avalie continuamente o desempenho das práticas e das pessoas, garantindo a eficiência da organização. Um método de acompanhamento das metas pré-definidas pela organização é o *Balance Scorecard*. Esse processo permite criar sinergia

entre as pessoas, assegurar que a estratégia seja implementada e avaliar o desempenho da organização.

Como todos os modelos de gestão, o CobiT prevê processos para garantir a melhoria contínua dos processos implantados. A metodologia de melhoria contínua Six-sigma pode ser adotada para atender essa exigência. O Six-sigma está baseado no PDCA (*Plan-Do-Control-Act*) do Deming.

Resumindo, as organizações de TI devem adotar um modelo de governança de TI para aumentar sua eficiência e demonstrar que podem agregar valor ao negócio. O CobiT é um modelo de gestão de TI reconhecido internacionalmente que define 34 processos de gestão que podem ser implantados utilizando práticas de processos de modelos de gestão específicos. É importante atingir o nível de maturidade de governança de TI compatível com as necessidades dos processos de negócio.

Mais informações

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