



Estrutura do Modelo Cobit

Prof. Sergio Nascimento

sergio.onascimento@sp.senac.br

Introdução

Como você estudou nas aulas anteriores, para muitas organizações a informação e a tecnologia que a suporta representam o seu bem mais valioso. Organizações bem-sucedidas reconhecem os benefícios da tecnologia da informação e entendem e gerenciam os riscos associados, tais como as crescentes demandas regulatórias e a dependência crítica de muitos processos de negócios da TIC.

Como foi visto na Aula 7, a Governança de TIC é de responsabilidade dos executivos da organização, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TIC contribua para atingir os objetivos estratégicos, ao:

- fazer uma ligação entre as atividades de TIC, direcionadas às necessidades de negócios;
- organizar as atividades de TIC em um modelo de processos estruturado;
- identificar os mais importantes recursos de TIC a serem utilizados;
- definir os objetivos de controle gerenciais a serem considerados.



Introdução

A área de TIC tem a missão de gerar valor para o negócio em duas frentes, na inovação (investimentos em desenvolvimento de soluções que possam melhorar a eficiência dos processos de negócio) e na manutenção do que já foi instalado (suporte aos processos de negócio e o dia a dia das operações da infraestrutura). Esse valor gerado, bem como os riscos que a operação representa para o negócio e os controles necessários para essa monitoração constituem elementos essenciais para a Governança de TIC.

Dessa forma, o principal papel da Governança de TIC é instituir um conjunto de melhores práticas para que esse valor gerado pela área de TIC seja perceptível. A percepção de valor gerado pela TIC acontecerá na medida em que a organização maximize os benefícios desse investimento, e que se gere vantagem competitiva no mercado. Esse conjunto de melhores práticas para o gerenciamento de controles deve ser implementado, gerenciado e extrair o máximo de eficiência para a operação de TIC garantindo, ao mesmo tempo, a proteção das informações institucionais.

Nesse contexto, a proteção às informações será satisfeita por requisitos de qualidade e segurança, através da estrutura operacional resultante do investimento nos recursos de TIC (aplicativos, informações, infraestrutura e pessoas). O conjunto de melhores práticas que se destaca mundialmente para atender a todos esses requisitos é o Cobit.

Nesta aula vamos analisar o histórico do Cobit e seus objetivos.



Histórico do modelo

O Cobit (Control Objectives for Information and Related Technology) é um conjunto de melhores práticas, com foco em controles e orientado a processos, para se implementar Governança de TIC em uma organização. Foi criado em 1994 pela ISACF (Information Systems Audit and Control Foundation) ligado à ISACA¹ (Information Systems Audit and Control Association).

Em 1998 foi publicada a segunda edição, contendo revisões nos objetivos de controle e padrões para implementação.

Para a área de TIC ter sucesso em entregar os serviços requeridos pelo negócio, os executivos devem implementar um sistema interno de controles ou uma metodologia. O modelo de controle do CobiT contribui para essas necessidades ao:

- fazer uma ligação com os requisitos de negócios;
- organizar as atividades de TIC em um modelo de processos geralmente aceito;
- identificar os mais importantes recursos de TIC a serem utilizados;
- definir os objetivos de controle gerenciais a serem considerados.



Histórico do modelo

O Cobit representa um modelo de Governança de TIC estratégico, pois promove a ligação entre os objetivos de negócio e os objetivos de TIC, instituindo métricas e modelos de maturidade que são necessários para medir seu desempenho e o quanto se está caminhando em direção ao atingimento dos objetivos. O Cobit tem orientação a processos, trazendo um conjunto de 34 processos de TIC que encerram todas as atividades possíveis para a TIC de uma organização, tanto no nível estratégico como no operacional. Há quatro conjuntos de processos denominados domínios, responsáveis pelo planejamento de organização de uma área de TIC, pelo universo das soluções automatizadas e sua operação, pela eficiência e segurança da operação de infraestrutura e pela medição dos resultados da TIC e o posicionamento da organização frente a fatores externos, como o ambiente regulatório.

Resumidamente, os processos são a solução oferecida pelo Cobit para extrair o máximo de retorno sobre o investimento nos recursos de TIC, de forma a atender às demandas do negócio.

A busca por essa extração de valor deve passar por algumas etapas como quais controles devem ser priorizados e implementados a partir de cada processo, bem como políticas, procedimentos e planos de ação para desenvolvê-los de maneira estruturada, objetivando ao atingimento das metas de negócio e prevenindo contra eventos indesejados e ameaças externas.

A capacidade de reação de uma organização frente a situações adversas, que é chamada responsividade, deve ser aprimorada através da operação eficiente dos controles dos processos do Cobit. Para tal, existem no Cobit itens estratégicos denominados objetivos de controle.



Cobit - Áreas de Governança de TIC



As áreas-foco da Governança de TIC representadas no pentágono direcionam a estrutura de processos do Cobit. Cada processo tem maior ou menor afinidade com uma área-foco, independentemente do domínio em que se encontra. Por exemplo, o processo de Gestão de projetos está intimamente ligado com a Entrega de valor, em nível primário, mas tem uma ligação em nível secundário com a Gestão de riscos. O processo de Planejamento estratégico é diretamente vinculado ao Alinhamento estratégico, mas tem ligação com a Gestão de recursos. E assim por diante, resultando no fato que a estrutura do Cobit habilita frontalmente a Governança de TIC em todas as suas dimensões.

Uma significativa mudança deu-se em 2005, através da versão 4.0, na qual foram inseridas práticas ligadas a outros modelos internacionais, como o COSO (financeiro), o ITIL (gestão de serviços de TIC) e a norma ISO/IEC 17799 (hoje, família de normas ISO/IEC 27000), que tratam de Segurança da Informação. O público-alvo foi expandido, contendo agora não somente técnicos de TIC, mas também gestores, especialistas e auditores de TIC.



Objetivos de Controle

Os objetivos de controle são elementos para a construção do processo. Eles devem ser priorizados, implementados e operados pelos gerentes das operações de TIC e de negócios, sendo a máxima responsabilidade por esses resultados do CIO da Organização. Se bem selecionados e implementados, os controles vão direcionar a operação diretamente aos requisitos de Governança necessários para garantir transparência nos resultados, segurança e precisão nas informações geradas e eficiência nos processos.



Objetivo de controle é uma declaração **do que** se quer controlar (nível estratégico), ao passo que o **controle** constitui o procedimento operacional para atingir o objetivo de controle. No Cobit 4.1 existem 210 objetivos de controle distribuídos pelos processos, sendo que cada processo tem um conjunto exclusivo, ou seja, um objetivo de controle só aparece uma vez.

Um bom exemplo seria pensarmos em um objetivo de controle que declara que as informações devem ser salvaguardadas na forma de backups, a fim de estarem disponíveis em caso de um acidente ou imprevisto na operação da TIC. Já o controle seria o procedimento escrito de como se extrai o backup no caso de uma organização específica, descrevendo passo a passo a operação na ferramenta utilizada, se as mídias de backup são enviadas para guarda externa e de que forma, qual a periodicidade da extração do backup, qual o tempo de retenção das informações e assim por diante.

Cobit - Controles

Os controles implementados pelo Cobit podem ser operados e monitorados em três níveis:

- no nível da alta direção, em que os resultados reportados pelas áreas operacionais servirão de base para a tomada de decisões que poderão redirecionar esforços e comunicação para toda a organização, realinhando-os em relação às metas estratégicas e objetivos e políticas operacionais necessárias para a geração de vantagem competitiva ou reposicionamento no mercado;
- no nível dos processos de negócio, no qual os executivos de segundo escalão (a partir tanto de definições ou reposicionamentos advindos da alta direção) vão cuidar para que os sistemas aplicativos de TIC e sua operação no ambiente de infraestrutura tenham a máxima eficiência. Quando o nível de automação ainda é insuficiente, pode haver grande dependência de indivíduos para a execução dos processos, que demandam maior acompanhamento dessa liderança de segundo nível. Pode-se concluir que esse nível é a ponte entre o que a organização necessita frente ao que ela realmente produz;
- finalmente, o nível mais baixo de liderança (que são os gestores de equipes operacionais e de TIC) têm a função de gerir o dia a dia das equipes de desenvolvimento, operação e suporte, e que extraem e analisam as métricas de desempenho sobre as quais os resultados serão apurados e transformados de forma a serem corretamente interpretados pela alta direção da organização. Se esse nível tiver um desempenho fraco, a operação de TIC terá baixa eficiência, o que trará riscos significativos ao atingimento das demandas de negócio. Por exemplo, um gerenciamento de mudanças insatisfatório poderia prejudicar (acidental ou deliberadamente) a confiança depositada em testes de integridade realizados nos sistemas.

Cobit - Controles



Os controles gerais são controles inseridos nos processos de TIC e serviços. Como exemplo, citamos:

- desenvolvimento de sistemas;
- gerenciamento de mudanças;
- segurança;
- operação de computadores.

Os controles inseridos nos aplicativos de processos de negócios são comumente chamados de controles de aplicativos. Exemplos:

- totalidade;
- veracidade;
- validade;
- autorização;
- segregação de funções.

Cobit - Objetivos do Modelo

O principal objetivo do modelo do Cobit é buscar a maximização do retorno dos investimentos que a empresa realiza nos recursos de TIC, alinhados às metas estratégicas da empresa.

Os recursos de TIC são:

- **aplicações:** são sistemas desenvolvidos pela área de TIC para automatizar os processos de negócio da organização, gerando valor em inovação e em eficiência das operações;
- **informação:** é o dado ou conjunto de dados que encerram significado para o negócio, portanto, tem valor estratégico e necessitam de proteção quanto a seu sigilo e precisão;
- **infraestrutura:** é o conjunto de recursos tecnológicos que compreendem uma gama de elementos (sejam *hardware*, *software* operacional, periféricos, ambientes operacionais e instalações) sobre o qual a organização realiza investimentos buscando retorno em termos de eficiência para o negócio;
- **pessoas:** são o recurso mais complexo e desafiador, no qual a organização investe na contratação, retenção e promoção e que

Cobit - Objetivos do Modelo

Através das áreas-foco da Governança de TIC, o Cobit provê uma metodologia para assegurar que:

- a área de TIC esteja alinhada com os negócios;
- a área de TIC habilite o negócio e maximize os benefícios;
- os recursos de TIC sejam usados responsavelmente;
- os riscos de TIC sejam gerenciados apropriadamente.

Como consequência direta, a utilização do Cobit permite à organização:

- otimizar investimentos habilitados por TIC;
- estabelecer relacionamento entre os processos de TIC e os requisitos de negócios;
- organizar as atividades de TIC em modelos de processos aceitos amplamente;
- identificar os principais recursos de TIC a serem valorizados;
- definir os objetivos de controle mais relevantes a serem implementados.

Cobit – Medição de Desempenho

A medição de desempenho é uma tarefa imprescindível para o sucesso da Governança de TIC. O Cobit é inteiramente voltado para essa tarefa. Todos os processos refletem métricas para medir o que os processos precisam entregar. Os processos conduzem a que se tenha transparência nos custos, valor e risco da TIC, e também no posicionamento, quando cabível, do negócio da organização frente a demandas legais e regulatórias. De nada adianta a organização ter resultados excelentes do ponto de vista da produção, se as leis e os regulamentos aplicáveis não estão sendo respeitados – o que pode resultar em multas que afetem os resultados no final de um exercício.

O papel da alta direção nessa empreitada é de fundamental importância para o sucesso da organização. O alinhamento estratégico entre as áreas de negócio, operacionais e de TIC é cada vez mais decisivo para que os planos de negócios possam ser executados de forma a promover as melhorias necessárias e garantir a capacidade de adaptação e de mudança que as organizações necessitam nesse mercado competitivo. Nesse sentido, algumas questões merecem análise profunda:

- Qual o posicionamento em relação aos nossos concorrentes?
- Quais as melhores práticas utilizadas no mercado e como estamos em relação às suas adoções?
- Uma vez que escolhemos as melhores práticas, qual a melhor forma de implementá-las de forma a gerar vantagem competitiva?
- Como melhorar o desempenho da TIC de forma que cada vez mais a preocupação da alta direção gire em torno de qualidade de entrega e não somente de desempenho?
- Como otimizar os processos de TIC de forma a garantir o máximo aproveitamento dos recursos humanos e tecnológicos envolvidos?

Cobit – Características e Objetivos



O CobiT é um modelo e uma ferramenta de suporte que permite aos gerentes suprir as deficiências com respeito aos requisitos de controle, questões técnicas e riscos de negócios, comunicando esse nível de controle às partes interessadas. O CobiT habilita o desenvolvimento de políticas claras e boas práticas para controles de TIC em toda a empresa, sendo atualizado continuamente e harmonizado com outros padrões e guias. Assim, tornou-se o integrador de boas práticas de TIC e a metodologia de Governança de TIC, que ajuda

A estrutura de processos do CobiT e o seu enfoque de alto nível orientado aos negócios fornecem uma visão geral de TIC e das decisões a serem tomadas sobre o assunto.

Considerações finais

Portanto, pode-se concluir que o Cobit foi criado, a princípio, como um guia para unificar a operação de TIC com uma visão de controles e evoluiu de maneira significativa na medida em que a informação passou a ser compreendida como um valioso ativo dentro das organizações, talvez o de maior valor no contexto atual. O Cobit evoluiu através dos anos, chegando às versões 4.0 e 4.1, quando passou a ser utilizado mundialmente, principalmente alavancado pela promulgação, implementação e auditorias dos elementos regulatórios previstos na Lei Sarbanes-Oxley, conforme estudamos na Aula 8. A orientação para negócios é o principal tema do CobiT, o qual foi desenvolvido não somente para ser utilizado por provedores de serviços, usuários e auditores, mas também, e mais importante, para fornecer um guia abrangente aos executivos e donos de processos de negócios.

O modelo do Cobit é baseado em prover a informação de que a organização precisa para atingir os seus objetivos, as necessidades para investir, gerenciar e controlar os recursos de TIC usando um conjunto estruturado de processos para prover os serviços que disponibilizam as informações necessárias para a organização.

O gerenciamento e o controle da informação estão presentes em toda a metodologia do CobiT e ajudam a assegurar o alinhamento com os requisitos de negócios.

A visão de processos permite que a organização procure a otimização do investimento em TIC, buscando a realização dos benefícios do investimento em recursos de TIC, sempre direcionados ao atingimento das metas estratégicas.

A versão 4.1 do Cobit foi amplamente divulgada e implementada em empresas de todo o mundo, alavancada pela promulgação da Lei Sarbanes-Oxley em 2002. As auditorias realizadas sob o escopo da SOX têm diversos aspectos que abordam a área de TIC e o Cobit 4.1 é utilizado nessas auditorias, o que obriga as empresas a também adotá-lo, para que “se fale a mesma língua”.

Nas próximas aulas estaremos aprofundando o estudo do Cobit 4.1 em toda a sua extensão e profundidade, para a implementação da Governança de TIC nas empresas.

Referências

FERNANDES, A. A.; ABREU, V. F. **Implantando a governança de TIC**: histórico do modelo. Rio de Janeiro: Brasport, 2012a.

_____. **Implantando a governança de TIC**: objetivos do modelo. Rio de Janeiro: Brasport, 2012b.

IT GOVERNANCE INSTITUTE. **COBIT 4.1**. USA: Rolling Meadows, 2007.