



Estrutura do Modelo Cobit

Prof. Sergio Nascimento

sergio.onascimento@sp.senac.br

Introdução

O CobiT é um *framework* mundialmente conhecido e utilizado em organizações de diversas naturezas e tamanhos. Em sua versão 4.1, o Cobit se apresenta como uma abrangente solução para a implementação da Governança de TIC, tendo sua estrutura totalmente orientada a processos.

O Cobit representa uma metodologia voltada a controles, mas orientada a processos, para um público-alvo diversificado dentro das organizações. Serve ao nível estratégico, habilitando uma gestão focada em metas e medição de resultados. Através de seus processos, possibilita a criação de políticas e procedimentos completos e focados em resultados. Pela medição de desempenho que proporciona, fornece ao negócio uma visão clara da contribuição da área de TIC e do retorno sobre o investimento realizado em seus recursos. Talvez o mais importante, habilita a organização a melhorar sua percepção sobre o valor gerado pela área de TICCC.

Nesta aula, vamos entender a estrutura do Cobit 4.1 em alto nível, ou seja, o modelo de processos, o módulo de avaliação e o módulo de implementação. Em aula futura, nos aprofundaremos na estrutura de um processo.

Devido à abrangência e complexidade do Cobit 4.1, alguns conceitos reaparecem em diversas aulas, o que é feito de forma intencional, para solidificar o aprendizado e criar o contexto necessário para a aula em questão.



Modelo de referência de processos do Cobit 4.1

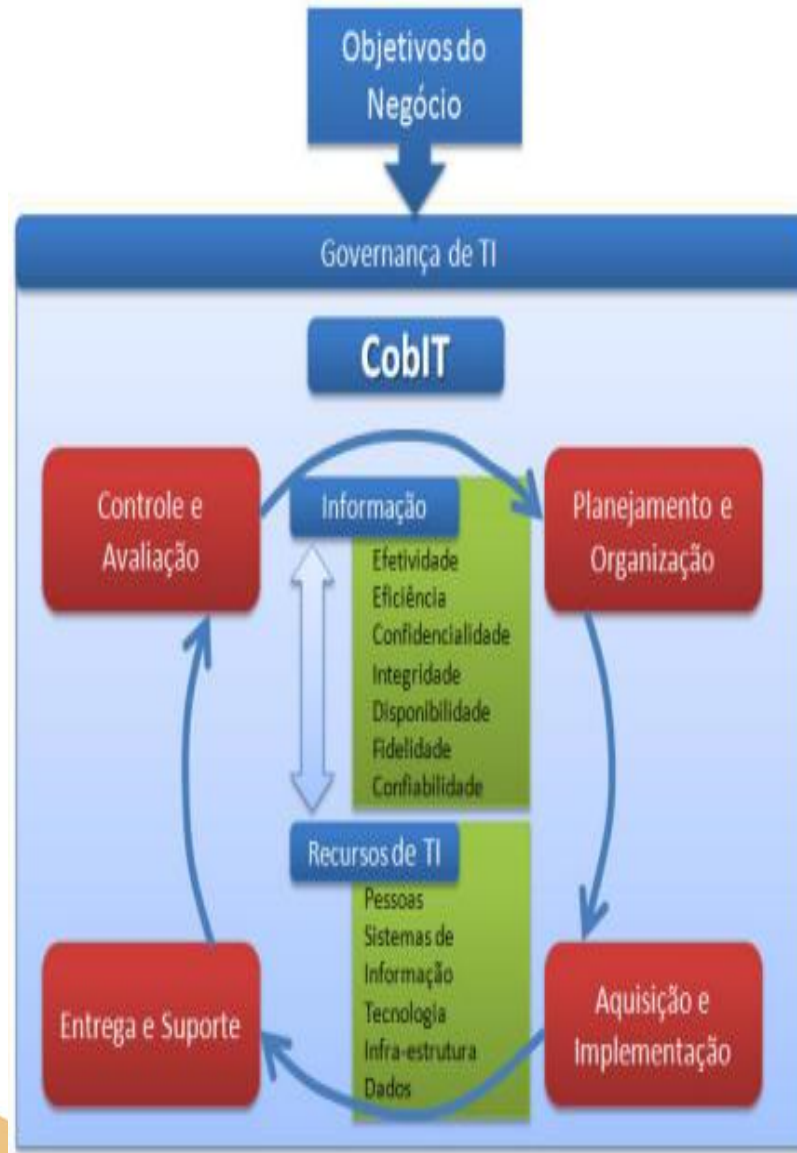
O modelo de processos do Cobit 4.1 apresenta quatro conjuntos de processos chamados domínios, a saber:



- **PO** (*Plan and Organize* – Planejar e Organizar)
- **AI** (*Acquire and Implement* – Adquirir e Implementar)
- **DS** (*Deliver and Support* – Entregar e Suportar)
- **ME** (*Monitor and Evaluate* – Monitorar e Avaliar)

Existem 34 processos do Cobit 4.1 e cada processo trata de um assunto da Governança de TIC. No entanto, os processos são interligados, alguns muito intimamente, e ao investir para a melhoria de um determinado processo, a organização estará promovendo a melhoria de um conjunto de processos.

Modelo de referência de processos do Cobit 4.1



- **PO (*Plan and Organize* – Planejar e Organizar)** – neste domínio encontram-se dez processos relativos à organização da área de TIC, como planejamento estratégico, arquitetura corporativa e estrutura e relacionamentos da área de TISCC, e também aspectos gerenciais, como gestão da qualidade, gestão de riscos e gestão de processos;



PO (Plan and Organize – Planejar e Organizar)

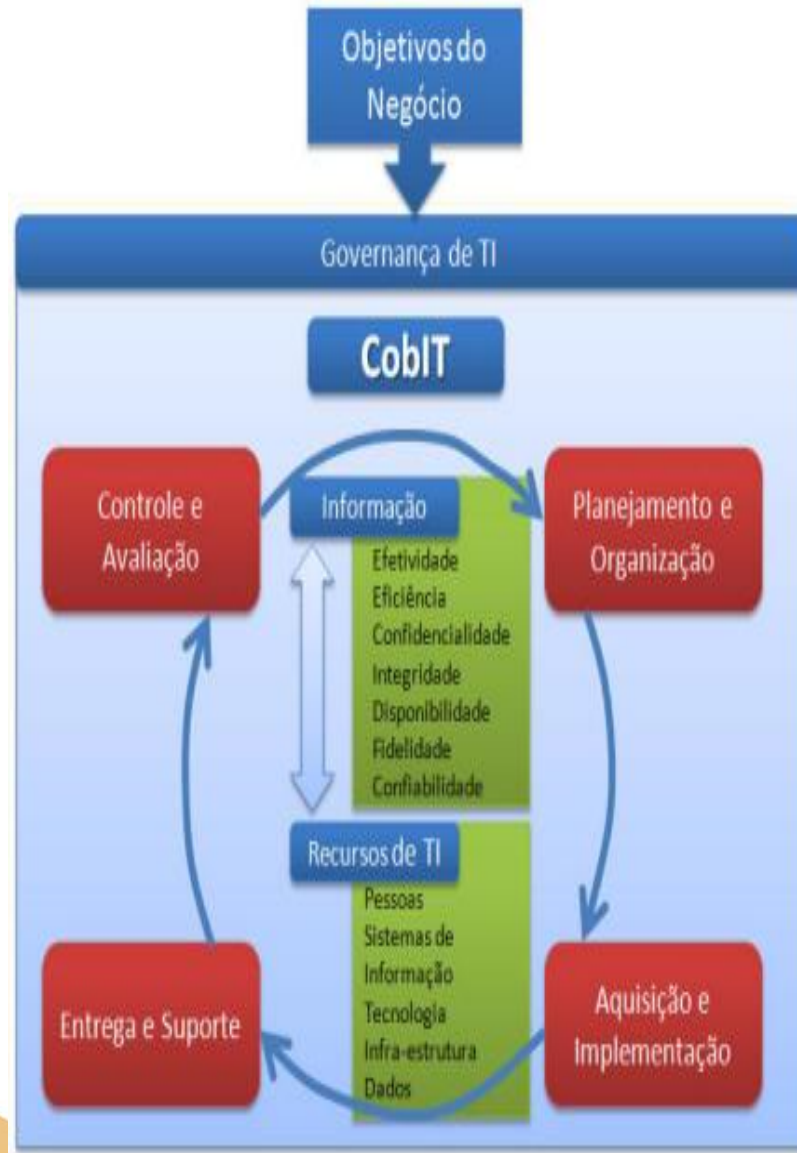
Esse domínio traz dez processos e para cada um deles, sua meta para gerar valor para o negócio:

- PO1 Definir um plano estratégico de TIC – incorporar TIC e gerenciamento de negócio na tradução dos requisitos de negócio em ofertas de serviços e no desenvolvimento de estratégias para entregar estes serviços de maneira eficaz e transparente;
- PO2 Definir a arquitetura da informação – estabelecer um modelo de dados de negócio que incorpore um esquema de classificação de dados para assegurar integridade e consistência de todos os dados;
- PO3 Determinar as diretrizes de tecnologia – definir e implementar um plano de infraestrutura, arquitetura e padrões de tecnologia que reconheça e aproveite as oportunidades tecnológicas;
- PO4 Definir os processos, a organização e os relacionamentos de TIC – estabelecer estruturas organizacionais de TICCC transparentes e responsivas. Definir e implementar processos de TIC com proprietários (de sistemas e dados), papéis e responsabilidades integrados aos processos de negócio e processos de decisão;
- PO5 Gerenciar o investimento de TIC – decidir o portfólio e investimentos em TICCC de forma eficaz e eficiente e elaborar e rastrear os orçamentos de TIC em linha com estratégias de TICCC e decisões de investimento;

PO (Plan and Organize – Planejar e Organizar) - continuação

- PO6 Comunicar metas e diretrizes gerenciais – fornecer políticas, procedimentos, diretrizes e outras documentações de forma precisa, compreensível e aprovada para as partes interessadas, incorporadas a uma estrutura de controles de TIC;
- PO7 Gerenciar os recursos humanos de TIC – admitir e treinar pessoal, motivar através de planos de carreira claros, atribuir funções coerentes com as habilidades, estabelecer um processo de revisão, criar descrições de cargos e assegurar a consciência da dependência de indivíduos;
- PO8 Gerenciar a qualidade – definir um sistema de gerenciamento de qualidade, monitorar continuamente o desempenho baseado em objetivos predefinidos e implementar um programa de melhoria contínua dos serviços de TIC;
- PO9 Avaliar e gerenciar os riscos de TICCC – desenvolver uma estrutura de gerenciamento de risco integrada às estruturas corporativa e operacional de gerenciamento de risco, avaliação, mitigação e comunicação de risco residual;
- PO10 Gerenciar projetos – aplicar aos projetos de TIC um programa definido e uma abordagem de gestão de projetos que permitam a participação das partes interessadas e a monitoração do andamento e dos riscos do projeto.

Modelo de referência de processos do Cobit 4.1



- **AI (Acquire and Implement – Adquirir e Implementar)** – são sete processos que tratam da aquisição ou desenvolvimento de aplicações e de infraestrutura e também do ciclo completo de uma mudança no ambiente de TIC (seja de uma aplicação ou de infraestrutura), contendo a preparação e a gestão da mudança, o planejamento e execução dos testes de homologação e a implementação no ambiente de produção;

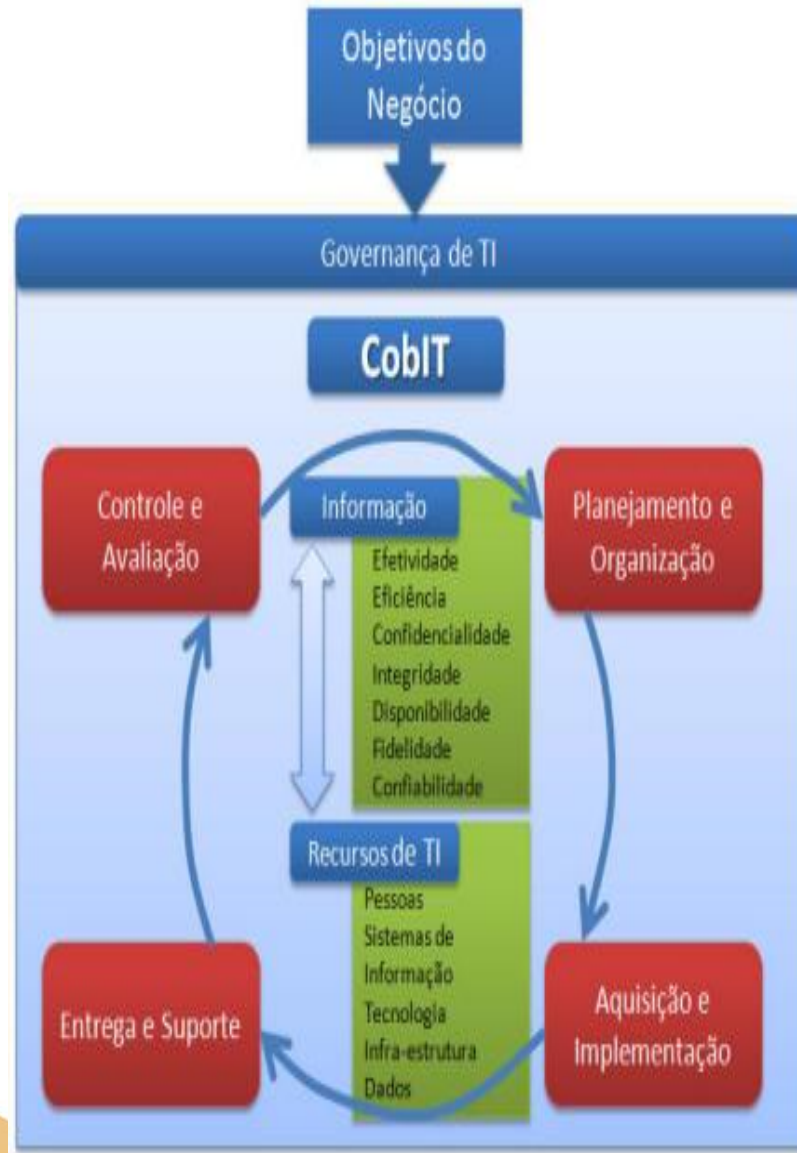


AI (Acquire and Implement – Adquirir e Implementar)

Esse domínio traz sete processos e para cada um deles, sua meta para gerar valor para o negócio:

- AI1 Identificar soluções automatizadas – identificar soluções tecnicamente viáveis e com boa relação custo-benefício;
- AI2 Adquirir e manter *software* aplicativo – assegurar a existência de um processo de desenvolvimento que contemple o cumprimento de prazos e otimização de custos;
- AI3 Adquirir e manter infraestrutura de tecnologia – disponibilizar plataformas apropriadas às aplicações de negócio, em alinhamento com a arquitetura de TIC definida e os padrões tecnológicos;
- AI4 Habilitar operação e uso – fornecer manuais de usuário, manuais operacionais e materiais de treinamento eficazes para transferir o conhecimento necessário à operação e uso bem-sucedidos do sistema;
- AI5 Adquirir recursos de TIC – adquirir e manter habilidades de TICCC que respondam à estratégia de entrega e a uma infraestrutura de TIC padronizada e integrada, e reduzir o risco de aquisição de recursos de TIC;
- AI6 Gerenciar mudanças – controlar a avaliação de impacto, autorização e implementação de todas as mudanças na infraestrutura, nas aplicações e nas soluções técnicas de TIC, minimizar erros devido a especificações de requisitos incompletas e interromper a implementação de mudanças não autorizadas;
- AI7 Instalar e homologar soluções e mudanças – testar se as aplicações e as soluções de infraestrutura atendem ao propósito pretendido e estão livres de erros, e planejar a implementação e a migração para produção.

Modelo de referência de processos do Cobit 4.1



DS (*Deliver and Support* – Entregar e Suportar) – contém 13 processos que tratam dos serviços de TIC e da gestão de sua infraestrutura, como a gestão dos acordos de nível de serviço, a gestão de fornecedores, planejamento de capacidade, continuidade, segurança de TISCC, gestão de incidentes e de problemas e gestão de operações em *data center*;



DS (Deliver and Support – Entregar e Suportar)

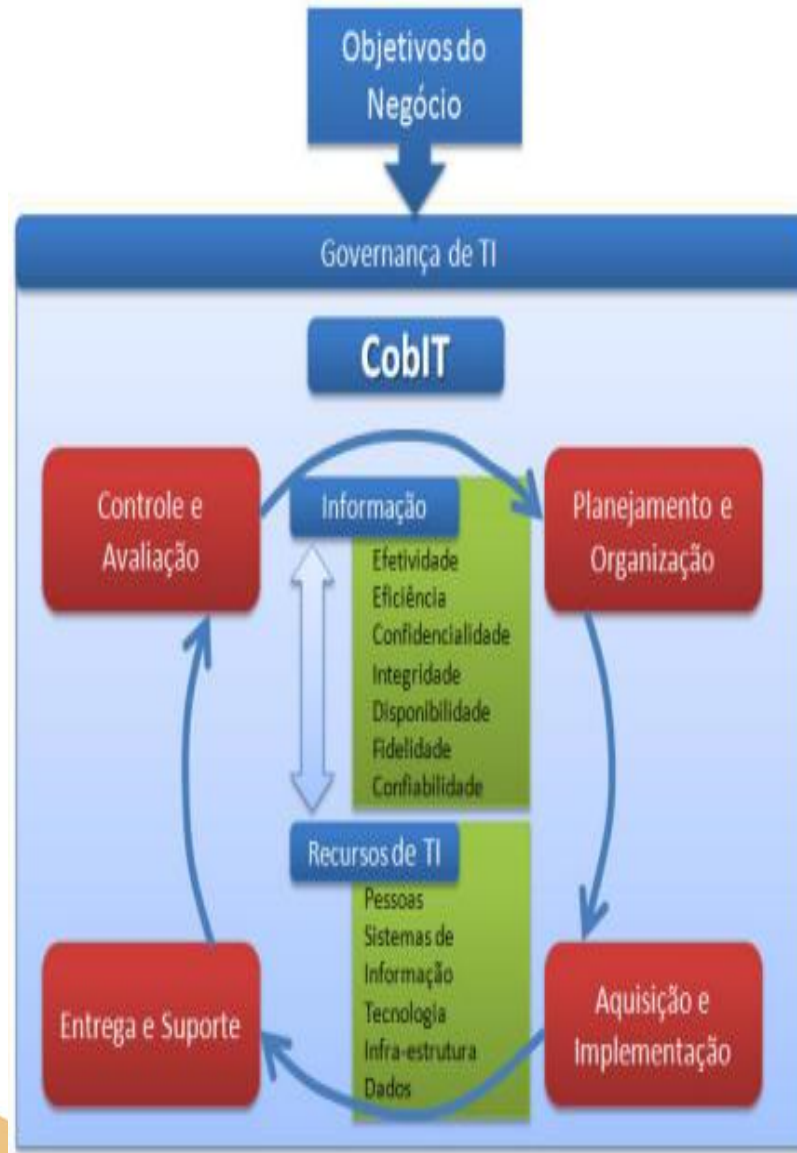
Esse domínio traz 13 processos e para cada um deles, sua meta para gerar valor para o negócio:

- DS1 Definir e gerenciar níveis de serviços – identificar os requisitos de serviço, acordar os níveis de serviço e monitorar o atendimento desses níveis de serviço;
- DS2 Gerenciar serviços terceirizados – estabelecer relacionamentos e responsabilidades bilaterais com prestadores de serviço terceirizados qualificados e monitorar a entrega dos serviços para verificar e assegurar o cumprimento dos acordos;
- DS3 Gerenciar o desempenho e a capacidade – atender aos requisitos de tempo de resposta dos diversos acordos de nível de serviço, minimizar o período de indisponibilidade e proporcionar melhorias contínuas no desempenho e na capacidade de TIC através de monitoramento e medição;
- DS4 Assegurar a continuidade dos serviços – incorporar a capacidade de recuperação em soluções automatizadas e desenvolver, manter e testar os planos de continuidade;
- DS5 Garantir a segurança dos sistemas – definir políticas, procedimentos e padrões de segurança de TICCC e monitorar, detectar, reportar e solucionar vulnerabilidades e incidentes de segurança;
- DS6 Identificar e alocar custos – coleta completa e precisa dos custos de TIC, um sistema de alocação justo aceito pelos usuários do negócio e um sistema de reporte oportuno do uso da TICCC e dos custos alocados;

DS (Deliver and Support – Entregar e Suportar) - continuação

- DS7 Educar e treinar os usuários – entender claramente as necessidades do usuário em termos de treinamento em TIC e executar uma estratégia eficaz de treinamento e medição dos resultados;
- DS8 Gerenciar a central de serviço e os incidentes – prover uma central de serviços profissional com respostas rápidas, procedimentos claros de escalonamento, análise de tendências e resolução;
- DS9 Gerenciar a configuração – estabelecer e manter um repositório preciso e completo de atributos e perfis mínimos de configuração de ativos e comparar com a configuração atual dos ativos;
- DS10 Gerenciar problemas – registrar, rastrear e resolver problemas operacionais. Investigar a causa-raiz de todos os problemas importantes e definir as soluções para os problemas operacionais identificados;
- DS11 Gerenciar os dados – manter a completude, a precisão, a disponibilidade e a proteção dos dados;
- DS12 Gerenciar o ambiente físico – prover e manter um ambiente físico adequado e que proteja os recursos de TIC contra acesso indevido, danos ou roubo;
- **DS13 Gerenciar as operações** – atingir os níveis de serviço operacionais para o processamento programado de dados, proteção das saídas de dados críticos, monitoramento e manutenção da infraestrutura.

Modelo de referência de processos do Cobit 4.1



- **ME (*Monitor and Evaluate* – Monitorar e Avaliar)** – traz quatro processos que se destinam à medição de desempenho e qualidade de aspectos operacionais como exigências regulatórias, controles internos, governança e resultados da área de TIC.



ME (Monitor and Evaluate – Monitorar e Avaliar)

Este domínio traz quatro processos e para cada um deles, sua meta para gerar valor para o negócio:

- ME1 Monitorar e avaliar o desempenho de TIC – monitorar e entregar relatórios sobre as métricas dos processos de TIC e identificar e implementar ações de melhoria de desempenho;
- ME2 Monitorar e avaliar os controles internos – monitorar os processos de controle interno de atividades de TIC e identificar ações de melhoria;
- ME3 Assegurar a conformidade com requisitos externos – identificar todas as leis, regulamentações e contratos aplicáveis e o respectivo nível necessário de conformidade de TICCC e otimizar processos de TIC, para reduzir o risco de não conformidade;
- ME4 Prover governança de TIC – preparar relatórios gerenciais sobre a estratégia, o desempenho e os riscos de TICCC e atender aos requisitos de governança em alinhamento com as diretrizes da alta direção.



Ao todo, portanto, existem 34 processos de TIC no Cobit 4.1. Pode-se notar que cada processo trata de um assunto da Governança de TIC. No entanto, os processos são interligados, alguns muito intimamente, e ao investir para a melhoria de um determinado processo, a organização estará promovendo a melhoria de um conjunto de processos.

O modelo de maturidade de processos

Um projeto envolvendo Cobit 4.1 em uma organização deve se iniciar por uma avaliação das condições atuais de um, alguns ou todos os processos. A avaliação é considerada como a capacidade de um processo de TIC em entregar valor ao negócio, em atendimento às metas estratégicas, de forma a maximizar o retorno dos investimentos sobre os recursos de TIC utilizados. Dessa forma, é necessário estabelecer um critério de avaliação (que se chama maturidade), uma escala, de forma a se oferecer uma nota em uma escala, uma ferramenta de medição (que se chama modelo de maturidade) e, a partir daí, se definir o que é necessário fazer para instituir a melhoria do processo até o estado desejado.



Esse método é conhecido como Gap Analysis – Análise de lacuna, em que o termo lacuna se refere à distância entre o estado desejado e o estado atual da maturidade do processo.

O modelo de maturidade de processos

Os modelos de maturidade são estruturas de avaliação de processos derivadas do modelo do CMMI, um *framework* especialista em desenvolvimento de sistemas. Foi definido a partir de um modelo genérico composto por seis atributos de maturidade, que são ações e produtos que devem incorporar a implementação de um processo. Esses atributos são os seguintes:

- comunicação e disseminação;
- políticas e procedimentos;
- objetivos e métricas;
- responsabilização;
- habilidades e competências;
- ferramentas e automação.



Considerando os níveis possíveis de 0 a 5, os modelos de maturidade foram construídos tendo em mente a implementação gradativa desses atributos, ligados ao assunto referente ao processo em questão.

Por exemplo, focando no processo de gestão de riscos, o modelo de maturidade correspondente trará no nível 0 afirmações que exprimem total ausência dos seis atributos e irá melhorando gradativamente, até que, no nível 5, exprima o estado da arte na prática de gestão de riscos.

O modelo de maturidade de processos

Através dos modelos de maturidade, a organização pode avaliar, através de seu próprio esforço ou então contando com o auxílio de consultorias externas, o exato estado atual de maturidade de suas práticas em relação aos 34 processos de TIC do Cobit. A partir dessa análise estabelece-se o nível de deficiências nos processos que merece ser alvo de um projeto de melhorias.

É importante frisar que o foco é a avaliação de maturidade, mas não necessariamente o funcionamento dos processos. Um processo pode ter maturidade alta, mas não gerar resultados confiáveis, pois o nível de aderência às práticas implementadas ainda não é satisfatório. Por exemplo, uma empresa pode ter investido na contratação e implementação de uma metodologia de gestão de projetos, definido responsabilidades, divulgado e treinado os executores do processo, estabelecido metas e métricas. Dessa forma, a maturidade está alta, ou seja, há potencial de que o processo se desempenhe a contento. No entanto, e com o tempo, após a implementação, os controles foram se afrouxando, houve substituição de pessoas que não receberam treinamento, o foco da organização passou a ser outro etc. Todos esses exemplos acabam por resultar em um funcionamento deficiente do processo e na utilização ineficiente dos recursos disponíveis. Para evitar esse efeito nocivo, são necessárias uma estrita monitoração e a realização de testes periódicos nos processos.

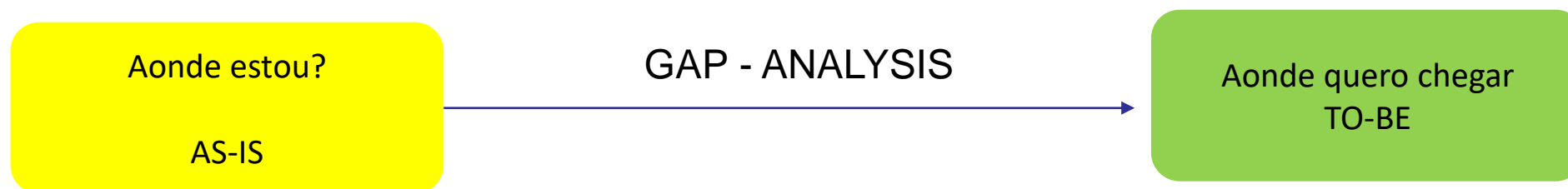


É importante frisar que a abrangência e profundidade com que os controles são implementados variam em função da natureza do negócio. Por exemplo, para uma instituição financeira internacional, as preocupações e demandas sobre a segurança das informações serão muito mais intensas do que em uma indústria de capital fechado. É fundamental estabelecer a dosagem correta de controles, um ajuste fino, que pode ser feito após a implementação dos processos.

O modelo de maturidade de processos

É importante destacar que as atividades desempenhadas dentro dos processos e controladas pelos objetivos e métricas disponíveis devem estar direcionadas aos objetivos estratégicos. Se uma empresa vende serviços de *e-commerce*, por exemplo, deve investir maciçamente em práticas que garantam a disponibilidade das aplicações em seu *site*. O negócio depende diretamente disso. Portanto, investir em melhorar a maturidade do processo de gestão de continuidade é fundamental para essa organização.

Enfim, o modelo de maturidade é uma importante ferramenta gerencial para a instituição e manutenção dos processos de Governança de TIC. O grau de controles que será ajustado através dessa ferramenta depende diretamente do negócio e do apetite a riscos que a organização está disposta a adotar, o que é uma decisão estratégica da alta direção.



Após identificar as lacunas nos processos, é necessário formular planos de ação para sua melhoria. Há métodos para auxiliar o nível decisório a estabelecer prioridades para investimentos na melhoria de processos, considerando aspectos de gestão de riscos, contribuição para as metas estratégicas e geração de vantagem competitiva para a empresa.

O modelo de maturidade de processos



De acordo com a natureza do negócio desenvolvido pela organização, sua dimensão, a dependência de tecnologia e de fatores externos, como o ambiente legal e regulatório, é possível com a ajuda do Cobit estabelecer mapas de risco e decisões estratégicas para quais processos serão prioritários para investimento.

Uma vez definida a prioridade de investimento, forma-se um escopo de projeto contendo os planos de ação para aqueles processos mais importantes. Esses planos de ação serão transformados em projetos, com definição de escopo, prazo, orçamento, recursos, responsabilidades e todos os outros componentes da gestão de projetos.

As ações a serem executadas nesses projetos são derivadas do conteúdo dos processos do Cobit, o que será objeto específico de estudo em aula futura. Nesse momento, vamos apenas entender que o nível de implementação dos processos do Cobit 4.1 está em uma ferramenta *web* denominada CobiT Online.

Considerações finais

Podemos concluir que o Cobit 4.1, ao se apresentar sob a forma de um modelo de processos, fornece uma solução estruturada e abrangente para a implementação de práticas de governança de TIC, aplicável a organizações de todos os tamanhos e segmentos de mercado.

O modelo do Cobit traz 34 processos agrupados em quatro domínios cobrindo todos os assuntos correlatos ao planejamento e organização de uma área de TIC, às práticas de aquisição, desenvolvimento e implementação de soluções sistêmicas e de infraestrutura, à entrega e suporte dos serviços prestados pela TIC e da monitoração de desempenho e qualidade dos processos de TICCC frente a controles internos e demandas regulatórias.

Em linhas gerais, entendemos que um projeto de Cobit se inicia com a avaliação do estado atual de um conjunto ou de todos os processos, a definição daquilo que é necessário se fazer para atingir os resultados esperados e com a montagem do projeto de melhorias, a partir de priorizações do que é mais relevante para a empresa.

A partir daí, é necessário gerenciar e executar a implementação dos controles e monitorar os resultados.

Referências

FERNANDES, A. A.; ABREU, V. F. **Implantando a governança de TIC**: diretrizes de Implementação. Rio de Janeiro: Brasport, 2012a.

_____. **Implantando a governança de TIC**: o modelo de referência de processos do CobiT 4.1. Rio de Janeiro: Brasport, 2012b.

_____. **Implantando a governança de TISCC**: o modelo de maturidade de processos. Rio de Janeiro: Brasport, 2012c.

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