

COBIT 5 – Governança, Gestão e Segurança da Informação

Por Sérgio Nunes Siqueira Júnior e Vanessa Leite
{sergio.nunes, vanessa.leite}@defenda.com.br

Introdução

O COBIT 5 é um grande avanço da ISACA na Governança da Tecnologia da Informação (TI). Com 15 (quinze) anos de aplicação em mercados globais, riscos, segurança da informação e auditoria, a nova versão do COBIT evoluiu junto com as reais necessidades estratégicas das organizações, auxiliando gestores a manter o equilíbrio entre três pilares: benefício, risco e custo.

Na versão 5 do COBIT são incorporadas as últimas novidades na governança dos serviços de TI e as técnicas de gerenciamento. O objetivo é agregar valor ao negócio através da TI e aumentar a confiança dos stakeholders no retorno sobre seus investimentos.

Governança da T.I

A informação é o recurso chave de toda organização, e faz com que a busca do negócio em extrair o mais alto valor das informações, impulse a evolução em modelos de gestão e governança da Tecnologia da Informação (TI). Como resultados dessa busca, os executivos e suas organizações estão se esforçando cada vez mais para manter a qualidade da informação, através da aplicação confiável e eficiente da tecnologia de forma a oferecer suporte às decisões estratégicas do negócio, bem como gerar o tão desejado valor aos stakeholders.

O COBIT já é considerado por muitos como a ferramenta mais adequada para auxiliar os gestores no direcionamento de seus objetivos, pois foca na governança e gestão da TI.

COBIT 5

Lançado em Abril de 2012, O COBIT 5, integra o COBIT 4.1, Risk IT e os modelos de processo do Val IT 2.0, provendo uma visão ponto a ponto, na qual é considerada toda a empresa para orientar a governança e a gestão da informação ao mais alto nível de retorno sobre o investimento nos ativos de TI.

Empresas públicas ou privadas, de todos os tamanhos, e nos mais diversos setores de atividades podem se beneficiar com o COBIT 5.

Por prover um sistema ponto a ponto na organização são considerados: o negócio, as áreas funcionais da TI e as partes interessadas, sendo tanto internas quanto externas. Como é baseada em cinco princípios chaves para a governança e gestão de organizações da TI, essa versão propõe mudanças significativas, tais como os princípios da governança demonstrados na figura 1.

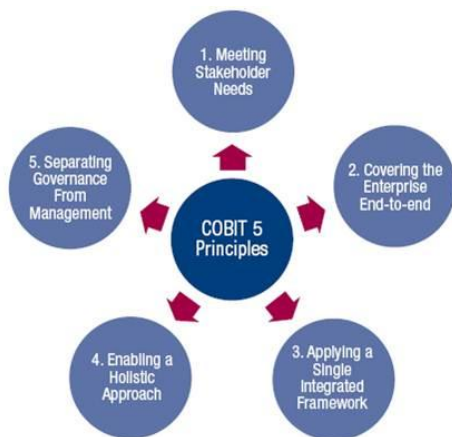


Figura 1 - Princípios de Governança

Os cinco princípios adotados na nova versão do framework são:

Princípio 1 - **Reunir as necessidades dos Stakeholders** – O COBIT 5 provê todos os processos requeridos e outros facilitadores para suportar a criação de valor ao negócio;

Princípio 2 – **Cobrir a organização fim-a-fim** – Abranger todas as funções e processos dentro da organização, tratando informação e tecnologia como ativos que precisam ser negociados como qualquer outro bem dentro da empresa;

Princípio 3 – **Aplicando um framework único e integrado** – Framework que deve estar alinhando com outras normas e melhores práticas e que sirva como padrão geral para a governança da TI corporativa.

Princípio 4 – **Aplicar uma abordagem holística** – Definir um conjunto de facilitadores para apoiar a implementação de uma governança global e um sistema de gestão da TI corporativo.

Os facilitadores (Enablers) são definidos como qualquer coisa que possa ajudar a alcançar os objetivos da organização.

O COBIT 5 define as seguintes categorias de facilitadores:

- Princípios, políticas e frameworks;
- Processos;
- Estruturas organizacionais;
- Cultura, ética e comportamento;
- Informação;
- Serviços, infraestrutura e aplicações; e
- Pessoas, habilidades e competências.

O detalhamento desses facilitadores pode ser encontrado na documentação do COBIT 5 framework.

Princípio 5 – **Separando Governança de Gerenciamento** – Duas disciplinas que englobam diferentes tipos de atividades, dessa forma, exigindo diferentes estruturas organizacionais e servindo a diferentes objetivos dentro da organização.

COBIT 5 e COBIT 4.1

Como esperado algumas mudanças ocorreram para que o COBIT evoluísse e atendesse as necessidades das organizações. Em resumo, as principais mudanças podem ser identificadas, na inclusão dos princípios fundamentais citados anteriormente, no foco nos facilitadores, e nas novas métricas e objetivos que foram adicionados.

Outras mudanças também ocorreram no modelo de RACI chart, e no processo de modelo de maturidade¹ e avaliação que, agora são baseados na ISO/IEC 15504 – Avaliação de Maturidade e Capacidade de Processos e no COBIT Assessment Programme 1.

¹. Vantagens do uso de Modelos de Maturidade foram discutidas no artigo no mês de Julho/12 de título Maturidade em Segurança da Informação.

De todas as mudanças ocorridas, talvez a mais significativa dessa versão, seja a distinção entre a governança e o gerenciamento da TI. Com essa nova distinção, torna-se indispensável à mudança de algumas atividades do COBIT.

Conforme essa nova definição a **Governança** é responsável por garantir que, as necessidades das partes interessadas, condições e opções, são avaliadas para determinar o equilíbrio de acordo com os objetivos da empresa. A direção é configurada através da priorização, tomada de decisão, monitoramento do desempenho e aderência as metas e objetivos da empresa.

O **Gerenciamento** é responsável por planejar, construir, executar e monitorar as atividades em alinhamento com a direção. Esse alinhamento é configurado pela governança, para garantir que sejam atingidos os objetivos da organização.

O equilíbrio entre essas duas áreas é fundamental para o atingimento dos objetivos acordados no planejamento estratégico da empresa através da TI.

COBIT 5 e Produtos Relacionados

A família de produtos do COBIT inclui além do framework, guias de implementação, detalhes dos facilitadores e utilização do COBIT em suporte à áreas específicas como, por exemplo, segurança e riscos.

Os seguintes produtos estão inclusos na última versão do COBIT 5:

- COBIT 5 (Framework);
- COBIT 5 Enabler guides;

Os facilitadores de governança e gerenciamento são discutidos em detalhes, incluindo:

- COBIT 5 Enabling process;
- COBIT 5 Enabling Information (em desenvolvimento);

- COBIT 5 professional guides;

No professional guides estão inclusos:

- COBIT 5 Implementation;
- COBIT 5 for Information Security;
- COBIT 5 for Assurance;
- COBIT 5 for Risk;
- Outros guias.

- Ambiente online colaborativo (*ambiente disponível para discussão do uso do COBIT 5*).

Considerações Finais

A utilização do COBIT 5 deve ser adaptada à empresa, para que seja possível atender às necessidades de cada organização. Com as novas definições e produtos, o COBIT 5 possibilita ajudar as empresas a controlar seus riscos através de uma adequada administração.

A última versão do COBIT está mais madura, principalmente na área de segurança da informação, começando a explorar oficialmente outras áreas, não somente com novos mapeamentos como a ISO/IEC 38500, mas com produtos oficiais em auditoria, risco e segurança da informação.

A governança e a gestão da informação e da tecnologia são assuntos cada vez mais complexos. Nesse cenário se faz necessário um alto grau de confiabilidade nas informações que irão auxiliar a atender os requisitos do negócio. O COBIT 5 é

utilizado como guia de negócios, e pode ajudar a contornar a complexidade da governança e gestão nas organizações, bem como aumentar a confiança nos sistemas de informações.

As mudanças ocorridas no COBIT 5, com a inclusão de requisitos mais específicos de segurança da informação, é um sinal de que cada vez menos é aceitável que empresas negligenciem seus riscos, uma vez que isso é considerado um fator crítico de sucesso para o atingimento dos objetivos do negócio.

Uma análise do nível de maturidade da organização baseada nos princípios básicos do COBIT pode ser um ponto de partida para o alinhamento da TI com o negócio.

Referências

[1] IT Governance Institute (ITGI). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.

[2] IT Governance Institute (ITGI). COBIT 4.1: Framework



Sérgio Nunes
Consultor de Segurança
da Informação.



Vanessa Leite
Consultora de Segurança
da Informação.