

Governança e Gerenciamento do COBIT

stecine.azureedge.net/repositorio/01640/index.html



OBJETIVOS

O COBIT

O COBIT(Do inglês, Control Objectives for Information and related Technology.) (Objetivos de Controle para a Informação e Tecnologia relacionada) apoia as organizações a alcançar as múltiplas necessidades da administração pela superação dos espaços entre os riscos de negócio, necessidades de controle e aspectos técnicos.

O COBIT é uma publicação elaborada pela **ISACA**, que, anteriormente, era conhecida como Information Systems Audit and Control Association, e atualmente, somente por sua sigla.

O COBIT foi desenvolvido como um recurso educacional para profissionais de TI da organização, sendo uma obra que não garante que seu uso parcial ou total impactará em resultados positivos e diretos para a organização, pois a utilização do COBIT deve ser adequada através do julgamento do profissional mediante as circunstâncias de segurança, risco, garantia e governança de TI apresentadas pelos sistemas ou ambientes de tecnologia da informação específicos.

ISACA

A ISACA é uma entidade sem fins lucrativos fundada em 1969 e reconhecida mundialmente por fornecer conhecimento, certificações, ações de comunidade, advocacia e treinamento em garantia e segurança de sistemas de informação (SI), governança corporativa e gestão de TI.

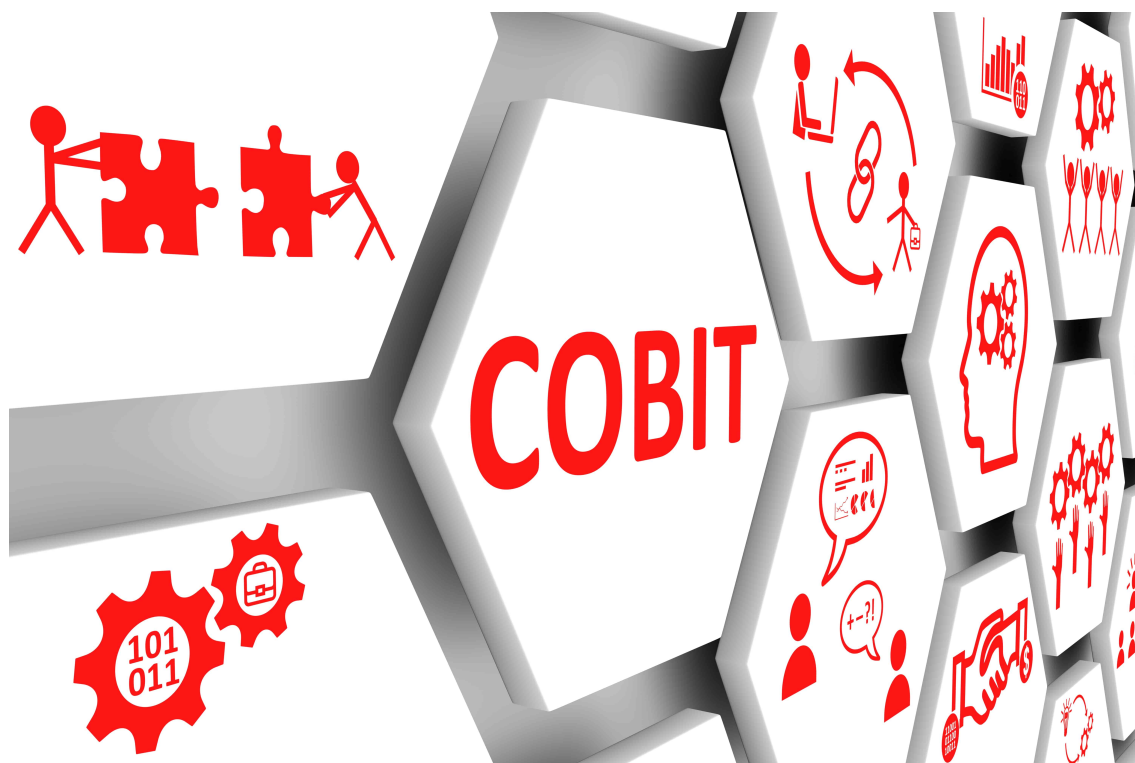


Imagem: Shutterstock.com

O principal objetivo do COBIT é proporcionar boas práticas para a organização através de um modelo de domínio e processos em uma estrutura lógica e gerenciável.


Atenção

As características do COBIT

O COBIT foi criado tendo como principais características:

Os benefícios do COBIT para a organização

São diversos os benefícios obtidos pela organização ao fazer uso do COBIT, entre os quais, podemos citar:





Você sabia?

Os princípios do COBIT

O COBIT possui foco em governança corporativa de TI e deixa clara a distinção entre governança e gestão. O COBIT está fundamentado em cinco princípios de governança corporativa de TI que permitem que a organização construa um framework efetivo de governança e gestão de TI, baseado em um conjunto holístico de habilitadores que otimizam investimentos em tecnologia e informação utilizados para o benefício das partes interessadas da organização.

A imagem abaixo apresenta os princípios do COBIT:



ISACA (2012, p.15), Adaptado por Isaac Barbosa.

Os princípios do COBIT.

Vamos conhecer cada princípio:

Atender às necessidades das partes interessadas

É extremamente importante entender o que as partes interessadas esperam da TI, quais as tecnologias relacionadas e quais as prioridades de modo a garantir criação de valor, por meio da TI, através do equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e da utilização dos recursos.

É importante transformar as necessidades das partes interessadas em estratégias corporativas.

Cobrir a empresa de ponta a ponta

O COBIT tem a função de integrar a governança corporativa de TI dentro da governança corporativa da organização, de modo a cobrir todas as funções e processos necessários para regular e controlar as informações da organização e tecnologias correlatas, onde quer que essas informações sejam processadas.

O COBIT não irá focar apenas nas funções de TI, mas também tratará as informações e tecnologias relacionadas como ativos que precisam ser tratados como qualquer outro ativo por todas as partes interessadas na organização.

Aplicar um framework único e integrado

O COBIT fornece um modelo único e integrado, pois é totalmente alinhado com outros padrões e modelos mais recentes, permitindo ser utilizado como principal integrador do modelo de governança e gestão da organização.

O modelo do COBIT fornece uma arquitetura simples para a estruturação dos materiais de orientação e produção de um conjunto consistente de produtos, sendo completo na cobertura da organização e fornecendo uma base consistente e eficiente para que seja facilmente integrado com outros modelos, padrões e práticas utilizados pela organização.

Permitir uma abordagem holística

O COBIT apoiará a governança e a gestão de TI, utilizando uma abordagem holística que envolverá a organização como um todo, incluindo seus componentes e suas inter-relações.

O COBIT define um conjunto de habilitadores que servem para apoiar a implementação de um sistema abrangente de gestão e de governança de TI da organização, sendo eles:

- Princípios, políticas e modelos;
- Processos;

- Estruturas organizacionais;
- Cultura, ética e comportamento;
- Informação;
- Serviços, infraestrutura e aplicativos;
- Pessoas, habilidades e competências.

Distinguir a governança da gestão

O modelo fornecido pelo COBIT torna transparente a distinção entre governança e gestão, pois estas duas áreas incluem diferentes tipos de atividades, estruturas e, também servem a diferentes propósitos.

A governança garantirá que as necessidades e as condições das partes interessadas sejam avaliadas com o objetivo de determinar as metas corporativas acordadas e equilibradas, enquanto a gestão consistirá em planejar, construir, executar e monitorar as atividades alinhadas com a estratégia definida pela governança, para que os objetivos da organização sejam concretizados.

Os domínios do COBIT

O COBIT é organizado em processos de governança e de gestão. Os processos de governança são cinco e estão organizados em um único domínio. Já os processos de gestão são 32 e estão organizados em quatro domínios (ISACA, 2012).

Os domínios do COBIT são os seguintes:

A imagem a seguir apresenta uma visão geral dos domínios e dos processos do COBIT que estudaremos:

ISACA (2012, p.35), adaptado por Isaac Barbosa.

Modelo de referência de processo do COBIT 5.



Os processos de governança

Os processos de governança asseguram que as necessidades, condições e opções das partes interessadas sejam avaliadas para que se determine os objetivos de negócio a serem atingidos.

A governança define a direção da organização por meio da priorização e da tomada de decisão.

Os processos de gestão

Os processos de gestão consistem basicamente em planejar, construir, executar e monitorar todas as atividades que estiverem alinhadas com os objetivos estratégicos estabelecidos pela governança de TI, de modo que os objetivos de negócio da organização sejam atingidos.

Avaliar, Dirigir e Monitorar (EDM)

Este domínio atende a definição de um framework de governança, das responsabilidades em termos de valor para a organização, fatores de risco, recursos e transparência da TI para todas as partes interessadas — *Stakeholders*.

Os processos do domínio EDM

Os processos de governança deste domínio ditam as responsabilidades da alta direção para a avaliação, direcionamento e monitoração do uso dos ativos de TI para a criação de valor para a organização, sendo eles:

1

EDM01 - Garantir a definição e manutenção do modelo de governança

Este processo define tudo que é necessário para analisar e articular os requisitos para a governança corporativa de TI. Também é responsável por colocar em prática e manter estruturas, princípios e processos, com clareza de responsabilidades e autoridade para alcançar a missão, as metas e os objetivos da organização.

EDM02 – Garantir a realização de benefícios

Este processo define tudo que é responsável por otimizar a contribuição de valor para o negócio a partir dos processos de negócios, serviços e ativos de TI resultantes de investimentos realizados pela TI a custos aceitáveis.

2

3

EDM03 – Garantir a otimização do risco

Este processo é responsável por assegurar que o apetite e tolerância a riscos da organização sejam compreendidos, articulados e comunicados, e que o risco ao valor da organização relacionado ao uso de TI seja identificado e controlado

EDM04 – Garantir a otimização dos recursos

Este processo é responsável por assegurar que as capacidades adequadas e suficientes relacionadas à TI (pessoas, processos e tecnologia) estarão disponíveis para apoiar os objetivos da organização de forma eficaz e a um custo aceitável.

4

5

EDM05 – Garantir transparência para as partes interessadas

Este processo é responsável por assegurar que a medição e os relatórios de desempenho e conformidade da TI corporativa sejam transparentes para que os *Stakeholders* aprovem as metas, métricas e ações corretivas que se fizerem necessárias.

Modelo de capacidade de processo do COBIT

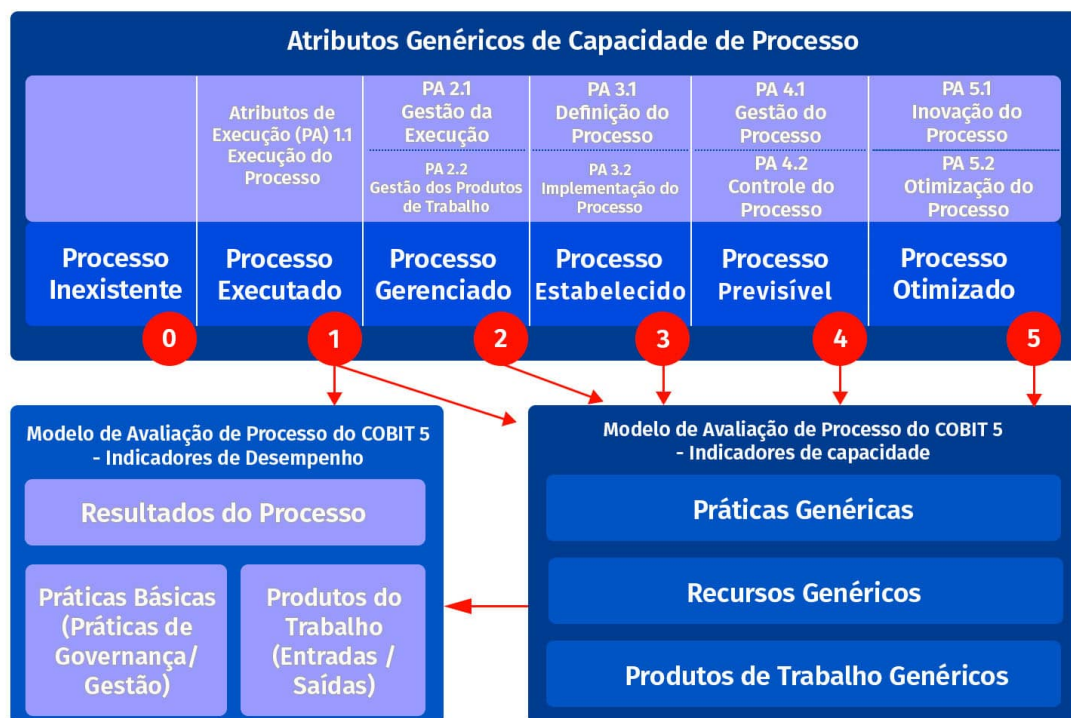
O COBIT possui um modelo para que a capacidade dos processos de TI de uma organização seja avaliada baseado na norma ISSO/IEC 15504 de engenharia de software (norma que avalia os processos). Este modelo do COBIT atende aos mesmos objetivos gerais de avaliações de processos e suporte de melhoria nos processos. Isso significa que o modelo fornecerá meios para que o desempenho dos processos de

governança (baseados no domínio EDM), ou processos de gestão (baseados em PBRM(Management Plan, Build, Run, and Monitor_)), possa ser medido, e o modelo ainda permitirá que as áreas da organização que necessitam de melhorias possam ser identificadas.

Todos os detalhes do modelo de avaliação da capacidade estão contidos na publicação *COBIT – Process Assessment Model (PAM): Using COBIT*.

Atenção

Para que tenhamos uma visão completa sobre o atual estado de governança da organização, é fundamental que outros habilitadores também sejam avaliados, conforme apresentado na imagem que traz um resumo do modelo de capacidade do COBIT:



ISACA (2012, p.44), adaptado por Isaac Barbosa.

Resumo do modelo de capacidade de processo do COBIT 5

De acordo com ISACA (2012):

Um processo poderá atingir seis níveis de capacidade e incluir uma designação, chamada de “processo incompleto”, caso as práticas sejam insuficientes para alcançar o objetivo completo do processo.

Os níveis são os seguintes:

Indica que o processo não foi implementado ou que seu objetivo não foi alcançado. Neste nível, há pouca ou quase nenhuma evidência de qualquer atingimento sistemático do objetivo do processo.

Indica que o processo implementado atingiu o seu objetivo.

Indica que o processo realizado é implementado de forma administrativa (planejado, monitorado e ajustado) e seus produtos de trabalho são adequadamente estabelecidos, controlados e mantidos.

Indica que o processo controlado foi implementado, utilizando um processo definido que é capaz de atingir os seus resultados.

Indica que o processo criado opera dentro dos limites definidos pela organização, para que os resultados positivos sejam gerados.

Indica que o processo previsível é melhorado de forma contínua e que estará sempre visando a concretização dos objetivos corporativos, atuais ou previstos pela organização.

Atenção

Alinhar, Planejar e Organizar (APO)

O domínio APO diz respeito à identificação de como a TI pode contribuir melhor com os objetivos de negócio. Processos específicos do domínio APO estão relacionados com a estratégia e táticas de TI, arquitetura corporativa, inovação e gerenciamento de portfólio, orçamento, qualidade, riscos e segurança.

Os processos do domínio APO

Os processos de gestão deste domínio tratam da forma como a TI pode contribuir de modo eficaz para os objetivos de negócio da organização. O domínio APO inclui, basicamente, os seguintes processos descritos a seguir:

APO01 – Gerenciar a Estrutura de Gestão de TI

Este processo é responsável por esclarecer e por manter a missão e visão da governança de TI da organização. O processo também é responsável por implementar e manter os mecanismos e autoridades responsáveis por gerenciar a informação e o uso da TI na organização.

APO02 – Gerenciar a Estratégia

Este processo é responsável por fornecer uma visão holística do negócio e do ambiente de TI atual na organização, qual é a direção futura e quais são as iniciativas necessárias para que se torne possível a migração para o ambiente futuro desejado pela organização.

APO03 – Gerenciar a Arquitetura da Organização

Este processo é responsável por estabelecer uma arquitetura comum, que consiste em processos de negócios, informações, dados, aplicações e tecnologia, para que se torne viável a realização de forma eficaz das estratégias de negócio e da TI da organização, por meio da criação de modelos e práticas-chave que descrevem a arquitetura de linha de base.

APO04 – Gerenciar Inovação

Este processo é responsável por manter uma consciência de TI e de tendências de serviços relacionados, identificar as oportunidades de inovação e planejar como se beneficiar da inovação com relação às necessidades do negócio. O processo também influenciará no planejamento estratégico e nas decisões de arquitetura corporativa da organização.

APO05 – Gerenciar Portfólio

Este processo é responsável por executar um conjunto de orientações estratégicas para que os investimentos da organização estejam alinhados com a visão de arquitetura corporativa. As características desejadas do investimento devem considerar as restrições de recursos e de orçamento. O processo também é responsável por avaliar, priorizar programas e serviços, gerenciar demandas dentro das restrições de recursos e de orçamento, com base no seu alinhamento com os objetivos estratégicos e riscos existentes na organização. Também serão movidos programas selecionados para o portfólio de serviços, para que ocorra a execução. Haverá o monitoramento do desempenho de todo o portfólio de serviços e programas, propondo qualquer ajuste que se faça necessário, em resposta ao programa e ao desempenho dos serviços ou mudanças de qualquer prioridade existente na organização.

APO06 – Gerenciar Orçamento e Custos

Este processo é responsável por administrar as atividades financeiras e de negócios relacionadas à TI, abrangendo o orçamento, a gestão de custos, os benefícios e a priorização dos gastos com o uso de práticas formais de orçamento e de um sistema justo e equitativo de alocação adequada de custos para a organização.

APO07 – Gerenciar Recursos Humanos

Este processo é responsável por fornecer uma abordagem estruturada, de forma a garantir a estruturação ideal, a colocação, os direitos de tomada de decisão e as habilidades dos recursos humanos. Ele também inclui o processo de comunicação dos papéis e responsabilidades definidas, planos de aprendizagem e de crescimento, e as expectativas de desempenho, com o apoio de pessoas competentes e motivadas da organização.

APO08 – Gerenciar Relacionamentos

Este processo é responsável por gerenciar o relacionamento entre o negócio e a TI de uma maneira formal e transparente, com o objetivo de garantir foco total na concretização dos objetivos comuns de todas as partes interessadas da organização.

APO09 – Gerenciar Contratos de Prestação de Serviços

Este processo é responsável por alinhar os serviços de TI e níveis de serviço com as necessidades e expectativas de todas as partes interessadas da organização. O processo inclui a identificação, a especificação, o projeto, a publicação, os acordos, o acompanhamento de serviços de TI, os níveis de serviço e os indicadores de desempenho.

APO10 – Gerenciar Fornecedores

Este processo é responsável por gerenciar os serviços relacionados a TI prestados por todos os tipos de fornecedores de modo que as necessidades de todas as partes da organização sejam atendidas de forma satisfatória. O processo também inclui a seleção de fornecedores, gestão de relacionamentos, gestão de contratos e a revisão e o monitoramento de desempenho de fornecedores de modo que seja totalmente garantida a efetividade e conformidade de acordo com as expectativas da diretoria executiva e de todas as partes interessadas da organização.

APO11 – Gerenciar Qualidade

Este processo é responsável por definir e comunicar todos os requisitos de qualidade em todos os processos, os procedimentos e os resultados das organizações, incluindo os controles necessários, o monitoramento contínuo e o uso de práticas eficientes e padrões na melhoria contínua e dos esforços que visam manter os níveis de eficiência desejados pela organização.

APO12 – Gerenciar Riscos

Este processo é responsável por identificar continuamente, avaliar e reduzir os riscos relacionados à TI dentro dos níveis de tolerância estabelecidos pela diretoria executiva da organização.

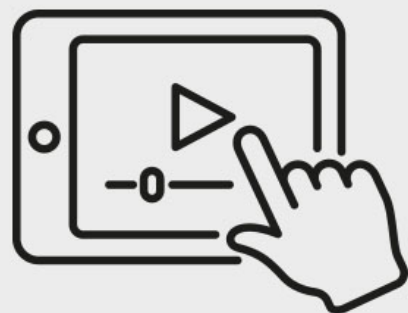
APO13 – Gerenciar Segurança

Este processo é responsável por definir, operar e monitorar um sistema para a gestão de segurança da informação da organização.

Domínios EDM (Avaliar, Dirigir e Monitorar) e APO (Alinhar, Planejar e Organizar)

O especialista Marcelo Vasconcellos Gomes apresenta um resumo dos principais processos dos domínios EDM e APO do COBIT. Assista!

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Verificando o aprendizado

1) Estudamos os principais benefícios que uma organização poderá ter ao fazer o uso do COBIT. Assinale a alternativa que apresenta um destes principais benefícios:

2) Qual dos domínios do COBIT inclui os processos de governança?

Gabarito

1) Estudamos os principais benefícios que uma organização poderá ter ao fazer o uso do COBIT. Assinale a alternativa que apresenta um destes principais benefícios:

A alternativa **"B "** está correta.

Com a utilização do COBIT, a organização poderá atingir um nível de excelência operacional por meio de aplicações confiáveis e eficientes, e, dessa forma, os processos serão otimizados reduzindo o custo dos serviços de TI.

2) Qual dos domínios do COBIT inclui os processos de governança?

A alternativa **"C "** está correta.

O domínio EDM atende a definição de um framework de governança, sendo composto por cinco processos de governança.

Avalie este módulo:

Para que a estratégia de TI seja realizada de modo a atingir os resultados esperados pela organização, e que estes resultados gerados estejam de acordo com as expectativas da diretoria executiva e de todas as partes interessadas da organização, as soluções de TI necessitam ser identificadas, desenvolvidas ou adquiridas, bem como implementadas e integradas aos processos de negócio da organização. Além disso, mudanças e a manutenção dos sistemas existentes deverão ser cobertas por este domínio a fim de garantir que as soluções propostas atendam às necessidades de negócio de forma contínua. Este domínio direciona as seguintes questões:

Os processos do domínio BAI

Os processos de gestão deste domínio são responsáveis por tornar concreta a estratégia de TI, de modo a identificar os requisitos necessários para a TI e gerenciar o programa de investimentos em TI.

Os processos deste domínio são os seguintes:

BAI01 – Gerenciar Programas e Projetos

Processo responsável por gerenciar de forma coordenada todos os programas e projetos do portfólio de investimentos da organização em alinhamento com as necessidades de negócio de todas as partes interessadas e da estratégia da organização. O processo também é responsável por iniciar, planejar, controlar e executar programas e projetos, e por uma revisão pós-implementação, de modo a garantir total qualidade no gerenciamento de programas e projetos da organização.

BAI02 – Gerenciar Definição de Requisitos

Processo é responsável por identificar soluções e analisar os requisitos antes da aquisição ou criação para assegurar que eles estarão em total conformidade com os requisitos estratégicos corporativos que cobrem os processos de negócio, aplicações, informações, questões de infraestrutura e de serviços. O processo também é responsável por assegurar a coordenação de todas as partes interessadas afetadas a revisão de opções viáveis, incluindo custos e benefícios, a análise de riscos e aprovação de requisitos e soluções propostas.

BAI03 – Gerenciar Identificação e Desenvolvimento de Soluções

Processo responsável por estabelecer e manter as soluções identificadas em conformidade com os requisitos da organização. Ele inclui o design, desenvolvimento, aquisição e terceirização e a parceria com fornecedores e vendedores. Também é realizada a gestão da configuração, o teste de preparação e outros testes que se façam necessários, manutenção dos requisitos de gestão e dos processos de negócio, controle de aplicações, gestão de dados, gerenciamento de infraestrutura e de serviços da organização.

BAI04 – Gerenciar Disponibilidade e Capacidade

Processo responsável por equilibrar as necessidades atuais e futuras de disponibilidade, desempenho e a capacidade de prestação de serviços de baixo custo da organização. O processo também inclui a avaliação das capacidades atuais, a previsão das necessidades futuras com base em requisitos de negócios, análise de impactos nos negócios e avaliação de riscos a fim de planejar e implementar ações para atender as necessidades identificadas pelas partes interessadas da organização.

BAI05 – Gerenciar Capacidade de Mudança Organizacional

Processo responsável por maximizar a probabilidade de implementar com sucesso uma mudança organizacional que seja de forma sustentável em toda a organização e de forma rápida e com risco reduzido, de modo a cobrir todo o ciclo de vida completo da mudança e de todas as partes interessadas e afetadas no negócio e na TI da organização.

BAI06 – Gerenciar Mudanças

Processo responsável por gerenciar todas as mudanças de maneira controlada, incluindo as mudanças nos padrões existentes e de manutenção de emergências relacionadas com os processos de negócio, aplicações e infraestrutura. O processo também inclui os padrões de mudança e procedimentos, avaliação de impacto, priorização e autorização, mudanças emergenciais, acompanhamento, elaboração de relatórios de acompanhamento, as fases de encerramento e de documentação.

BAI07 – Gerenciar Aceitação e Transição da Mudança

Processo responsável por aceitar e produzir formalmente novas soluções operacionais, incluindo o planejamento de implementação do sistema, a conversão de dados, testes de aceitação, o processo de comunicação, a preparação de liberação, a distribuição para produção dos processos de negócios e serviços de TI novos ou alterados, o suporte de produção e uma revisão pós-implementação de modo a garantir total qualidade no aceite e na transição da mudança na organização.

BAI08 – Gerenciar Conhecimento

Processo responsável por manter a disponibilidade de todo o conhecimento relevante para a organização, o conhecimento atual, o conhecimento validado e confiável de modo que todas as atividades do processo sejam suportadas e de modo a facilitar a tomada de decisão. O processo também inclui um plano para a identificação, coleta, organização, manutenção, utilização e extração correta do conhecimento.

BAI09 – Gerenciar Ativos

Processo responsável por gerenciar todos os ativos de TI através do seu ciclo de vida, de modo a assegurar que seu uso agregue valor a um custo ideal dentro da organização. O processo também garante que os ativos permaneçam operacionais e fisicamente protegidos. Também serão mantidos os ativos que são fundamentais para apoiar a disponibilidade e a capacidade dos serviços da organização.

BAI10 – Gerenciar Configuração

Este processo é responsável por definir e por manter as descrições e as relações entre os principais recursos e as capacidades necessárias para que os serviços de TI sejam prestados de forma eficiente. O processo também inclui a coleta de informações de configuração, o estabelecimento das linhas de base, a verificação e a auditoria das informações de configuração e a atualização do repositório de configuração da organização.

Entregar, Serviço e Suporte (DSS)

Este domínio é direcionado para a entrega real dos serviços requeridos, os quais incluem a entrega dos serviços, gestão da segurança e continuidade, serviço de suporte ao usuário e gestão dos dados e equipamentos operacionais. Ele direciona, tipicamente, as seguintes questões:

Os Processos do Domínio DSS

Os processos de gestão deste domínio se referem à entrega de todos os serviços de TI que são necessários para atender os planos táticos e estratégicos da organização. Os processos deste domínio são os seguintes:

1

DSS01 – Gerenciar Operações

Este processo é responsável pela coordenação e pela execução de todas as atividades e procedimentos operacionais necessários para que sejam entregues serviços de TI com qualidade, incluindo a execução de procedimentos operacionais,

padrões predefinidos e todas as atividades exigidas para garantir total qualidade nas operações da organização.

DSS02 – Gerenciar Solicitações e Incidentes de Serviços

Processo responsável por fornecer uma resposta rápida e eficaz a todos os tipos de solicitações dos usuários da operação e por garantir a resolução eficiente de todos os tipos de incidentes. O processo fornecerá todo o suporte necessário às solicitações dos usuários, registros de solicitações, investigação e diagnóstico necessários, escalonamento e solução de incidentes, de modo que seja garantida total disponibilidade dos serviços da organização.

2

3

DSS03 – Gerenciar Problemas

Processo responsável por identificar e classificar os problemas e suas causas e efeitos, de modo a fornecer resolução e prevenção de incidentes recorrentes. O processo também fornecerá todas as recomendações que forem necessárias para que sejam implementadas melhorias nos processos atuais da organização.

DSS04 – Gerenciar Continuidade

Este processo é responsável por estabelecer e manter um plano, de modo a permitir que a TI responda a incidentes e interrupções, a fim de permitir total continuidade na operação de processos críticos de negócios e serviços de TI necessários e manter a disponibilidade de informações em um nível aceitável para a organização.

4

5

DSS05 – Gerenciar Serviços de Segurança

Este processo é responsável por manter as informações protegidas da organização e por manter um nível de risco aceitável para a segurança da informação da organização, de acordo com as suas políticas de segurança. Também será garantida a manutenção das funções de segurança da informação, os privilégios de acessos e o monitoramento de segurança da organização.

DSS06 – Gerenciar Controles do Processo de Negócio

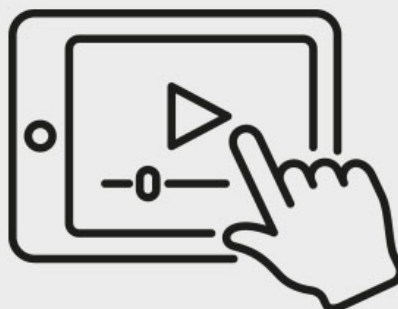
Processo responsável por definir e manter os controles de processo de negócio apropriados para assegurar que as informações relacionadas e processadas atendam a todos os requisitos de controle de informações relevantes existentes na organização.

6

Domínios BAI (Construir, Adquirir e Implementar) e DSS (Entregar, Serviço e Suporte)

O especialista Marcelo Vasconcellos Gomes apresenta um resumo dos principais processos dos domínios BAI e DSS do COBIT. Assista!

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Verificando o aprendizado

1) Qual a principal responsabilidade dos processos de gestão do domínio Construir, Adquirir e Implementar (BAI)?

2) Qual a principal responsabilidade dos processos de gestão do domínio Entregar, Serviço e Suporte (DSS)?

Gabarito

1) Qual a principal responsabilidade dos processos de gestão do domínio Construir, Adquirir e Implementar (BAI)?

A alternativa **"E "** está correta.

Este domínio tem como principal objetivo o fornecimento de processos de gestão que serão responsáveis por concretizar a estratégia de TI, tais como o “BAI01 – Gerenciar Programas e Projetos” e o “BAI02 – Gerenciar Definição de Requisitos”, além de outros processos de gestão.

2) Qual a principal responsabilidade dos processos de gestão do domínio Entregar, Serviço e Suporte (DSS)?

A alternativa **"D "** está correta.

Este domínio tem como principal objetivo o fornecimento de processos de gestão que serão responsáveis por garantir a entrega de todos os serviços de TI da organização, tais como o “DSS01 – Gerenciar Operações” e o “DSS02– Gerenciar Solicitações e Incidentes de Serviços”, além de outros processos de gestão.

Avalie este módulo:

Monitorar, Avaliar e Analisar (MEA)

Todos os processos de TI necessitam ser regularmente avaliados quanto a sua qualidade e conformidade com os requerimentos de controle. Tal domínio direciona a performance da gestão, o monitoramento dos controles internos, as conformidades regulamentares e fornece governança.

Este domínio direciona, tipicamente, as seguintes questões de gestão:

Os processos do domínio BAI

Os processos de gestão deste domínio têm como principal objetivo o de monitoramento de desempenho dos processos de TI, nos quais será avaliado se a execução dos processos está em conformidade com os objetivos e requisitos da organização.

Os processos deste domínio são:

MEA01 – Monitorar, Avaliar e Analisar Desempenho e Conformidade

Este processo é responsável pela coleta, validação e avaliação dos objetivos e métricas do processo de negócios e de TI da organização. Também será realizado o monitoramento a fim de garantir que os processos estão sendo executados conforme as metas, as métricas de desempenho e as conformidades acordadas. O processo também fornecerá informação eficiente e adequada para a organização.

Práticas deste processo:

- Estabelecer uma abordagem de monitoramento;
- Definir metas de desempenho e conformidade;
- Coletar e processar dados de desempenho e conformidade;
- Analisar e reportar desempenho;
- Assegurar a implantação de ações corretivas.

MEA02 – Monitorar, Avaliar e Analisar o Sistema de Controle Interno

Este processo é responsável por monitorar e avaliar continuamente o ambiente de controle, incluindo as autoavaliações e análises de avaliações independentes. O processo também permitirá a execução de melhorias por meio de uma gestão eficiente na identificação de ineficiências e deficiências nos controles atuais da organização.

Práticas deste processo:

- Monitorar controles internos;
- Revisar efetividade de controles de processos de negócio;
- Realizar autoavaliações de controles;
- Identificar e reportar deficiências de controles;
- Assegurar que provedores de garantia (auditoria) sejam independentes e qualificados;
- Planejar iniciativas de garantia (auditoria);
- Definir escopo de iniciativas de garantia (auditoria);
- Executar iniciativas de garantia (auditoria).

MEA03 – Monitorar, Avaliar e Analisar Conformidade com Requisitos Externos

Este processo é responsável por avaliar se os processos de TI e de negócios suportados pela TI estão em conformidade com as leis, regulamentos e exigências contratuais. O processo também obterá a garantia de que os requisitos foram identificados e respeitados, e que sejam integrados à conformidade com o cumprimento global da organização.

Práticas deste processo:

- Identificar requisitos de conformidade externos;
- Otimizar resposta a requisitos externos;
- Confirmar conformidade externa;
- Obter garantia de conformidade externa.

A importância do monitoramento

Para que a organização garanta que todos seus recursos sejam utilizados de forma eficiente, o monitoramento de TI é uma ferramenta indispensável para os negócios diretos de uma organização estratégica. A cada dia que passa, as organizações que não utilizam a tecnologia como ferramenta estratégia para impulsionar o seu negócio podem perder o mercado para o concorrente que é extremamente agressivo.

Metas e métricas relacionadas com a TI

O processo MEA01 descreve que devem ser realizadas todas as ações necessárias na organização de coleta, validação e avaliação do negócio, objetivos e métricas de processo e de TI. Os processos que estão sendo executados, de forma que o acordado no desempenho e nos objetivos de conformidade e métricas não esteja sendo atendido, deverão ser monitorados e, por meio do uso de relatórios e indicadores sistêmicos, a alta gestão da organização poderá tomar decisões estratégicas, de modo a definir ações que garantam total conformidade na execução dos processos.

As métricas possuem como objetivo principal o de apoiar a realização dos principais processos da organização relacionados com a TI.

Como exemplo de métricas, podemos citar:

	% dos processos críticos do negócio, serviços de TI e programas do negócio que são cobertos pela avaliação dos riscos.
Gerenciamento dos riscos de negócio relacionados a TI.	Número de incidentes significativos relacionados com a TI e que não foram identificados na avaliação dos riscos.
	% de avaliação de riscos, incluindo os riscos relacionados com a TI e a frequência de atualização do perfil do risco.
	Quantidade de interrupções nos processos de negócio devido a ocorrência de incidentes nos serviços de TI.
Entrega de serviços de TI alinhada com os requisitos dos negócios.	% das partes interessadas do negócio que estão satisfeitas com a entrega dos serviços de TI de modo que os acordos em níveis de serviço sejam atendidos.

	% de usuários satisfeitos com a qualidade da prestação de serviços de TI.
	Frequência da capacidade da maturidade e das avaliações de otimização dos custos.
Otimização dos ativos de TI.	Tendência da avaliação dos resultados.
	Níveis de satisfação dos executivos da organização com relação aos custos e capacidades do negócio.
	Quantidade de incidentes relacionados a inconformidades da política.
Conformidade da TI com as políticas internas da organização.	% de interessados que possuem conhecimento sobre as políticas.
	% de políticas suportadas por normas e práticas de trabalho eficazes.
	Frequência de revisão e atualização das políticas da organização.

Atenção! Para visualização completa da tabela utilize a rolagem horizontal

Monitoramento e fiscalização

Como todo processo presente no COBIT, a execução do processo MEA01 é realizada por meio de práticas que estão organizadas nos seguintes subprocessos:

Estabelecer uma abordagem para o monitoramento e fiscalização: este subprocesso tem como objetivo garantir o envolvimento de todas as partes interessadas da organização para que se estabeleça e se mantenha uma abordagem de monitoramento e de fiscalização, de modo a atingir os objetivos estratégicos da organização.

Conjunto de desempenho e de metas da conformidade: este subprocesso fornece um conjunto de desempenho e de metas para cada métrica de monitoramento e fiscalização que for determinada pela organização.

Recolher e processar dados de desempenho e de conformidade: este subprocesso é responsável por fornecer os mecanismos necessários para que se colete e se processe os dados de desempenho e de conformidade de cada métrica de monitoramento e fiscalização que for determinada pela organização.

Analisar e reportar o desempenho: este subprocesso é responsável por analisar e reportar o desempenho das métricas de monitoramento e fiscalização que foram determinadas pela organização. O reporte do desempenho deve ser claro e objetivo, de modo a atender às necessidades das partes interessadas da organização.

Garantir a aplicação de todas as ações corretivas que se fizerem necessárias: este subprocesso garante que todas as ações corretivas identificadas nos subprocessos anteriores sejam aplicadas nos processos da organização, de modo a desenvolver um ciclo de melhoria contínua.

O subprocesso MEA01.01, que estabelece uma abordagem para o monitoramento e fiscalização, é considerado uma das práticas que busca o envolvimento de todas as partes interessadas com o objetivo de estabelecer e manter uma abordagem de monitoramento capaz de definir os objetivos, escopo e método, com a intenção de medir a solução de negócios e de realizar a entrega de serviços que possam contribuir de forma efetiva e estratégica para a organização.

Esta abordagem deve ser integrada com o desempenho do sistema de gestão corporativo da organização.

As atividades desta prática são as seguintes:

baselines benchmarking

Baselines

É o valor mínimo ou ponto inicial utilizado para realizar comparações

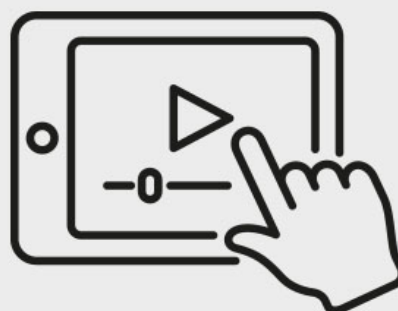
Benchmarking

É o processo de avaliação em relação à concorrência, e/ou produtos e serviços correlatos internos, por meio do qual a comparação destes resultados e métricas observadas/obtidas servem como base para aperfeiçoar seus métodos/processos.

Domínio MEA (Monitorar, Avaliar e Analisar)

O especialista Marcelo Vasconcellos Gomes apresenta um resumo dos principais processos do domínio MEA. Assista!

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



TÍTULO 1

Verificando o aprendizado

1) Estudamos conceitos importantes sobre o domínio Monitorar, Avaliar e Analisar (MEA). Dentre as questões que são direcionadas por este domínio, podemos citar:

2) Qual o processo do domínio Monitorar, Avaliar e Analisar (MEA) que é responsável pela coleta, validação e avaliação dos objetivos e métricas do processo de negócios e de TI da organização?

Gabarito

1) Estudamos conceitos importantes sobre o domínio Monitorar, Avaliar e Analisar (MEA). Dentre as questões que são direcionadas por este domínio, podemos citar:

A alternativa "**C**" está correta.

Todos os processos de TI necessitam ser regularmente avaliados quanto a sua qualidade e conformidade com os requerimentos de controle da organização. Dessa forma, é fundamental que se questione se a gestão está realmente garantindo que os controles internos sejam efetivos e eficientes.

2) Qual o processo do domínio Monitorar, Avaliar e Analisar (MEA) que é responsável pela coleta, validação e avaliação dos objetivos e métricas do processo de negócios e de TI da organização?

A alternativa "**A**" está correta.

Além da coleta, validação e avaliação dos objetivos do processo de negócio e de TI, o processo MEA01 também é responsável pelo monitoramento, a fim de garantir que os processos estão sendo executados conforme as metas, as métricas de desempenho e as conformidades acordadas. O processo também fornecerá informação sistemática e adequada para a diretoria executiva e todas as partes interessadas da organização.

Avalie este módulo:

Considerações Finais

Estudamos conceitos importantes sobre o COBIT, bem como seus princípios, características e benefícios. Entendemos os principais objetivos e os processos dos domínios EDM (Avaliar, Dirigir e Monitorar) e APO (Alinhar, Planejar e Organizar). Também compreendemos os principais objetivos e processos dos domínios BAI (Construir, Adquirir e Implementar) e DSS (Entregar, Serviço e Suporte). Além disso, reconhecemos a importância do domínio MEA (Monitorar, Avaliar e Analisar) e como seus processos podem garantir o monitoramento e a medição eficiente do desempenho dos processos de TI de uma organização eficiente.

Podcast

Ouça o podcast do especialista Marcelo Vasconcellos Gomes com o resumo do tema.

Para ouvir um *podcast* sobre o assunto, acesse a versão online deste conteúdo.



Avaliação do tema:

REFERÊNCIAS
