

Pré-Curso COBIT® 5 Foundation

Versão 01.02.br - ativo

Para feedback e comentários:
contato@mpplaza.com.br

Cobertura Parcial do Syllabus do COBIT5 Foundation

Use esse livro para se preparar para aula presencial
Material adicional para auxiliar seu aprendizado



Visit us on
Facebook

Management Plaza Brasil

Autor : Ernani Marques
Revisão : Ronielton Oliveira

Pré-Curso

Sumário

| | |
|---|------------|
| LISTA DE FIGURAS | III |
| MANUAL DE TREINAMENTO PRÉ-CURSO DO COBIT® 5 FOUNDATION | IV |
| 1. INTRODUÇÃO..... | 6 |
| 2. NOVIDADES DO COBIT 5..... | 6 |
| 3. PRINCÍPIOS..... | 6 |
| 3.1 Atender as necessidades das partes interessadas | 6 |
| 3.2 Abranger a empresa de ponta-a-ponta..... | 8 |
| 3.3 Aplicar um <i>framework</i> único e integrado | 9 |
| 3.4 Facilitar uma abordagem holística | 9 |
| 3.4.1 Dimensões de Facilitadores | 10 |
| 3.5 Separar a Governança da Gestão | 11 |
| 4. NOVO MODELO DE REFERÊNCIA DE PROCESSOS..... | 11 |
| 4.1 Processos de Governança..... | 12 |
| 4.2 Processos de Gerenciamento..... | 12 |
| 5. ESTRUTURA DE PROCESSOS..... | 13 |
| 6. CICLO DE VIDA DA IMPLEMENTAÇÃO..... | 14 |
| 7. MODELO DE CAPACIDADE DE PROCESSOS | 14 |
| 8. RESUMO DAS DIFERENÇAS COBIT 4.1 E COBIT 5..... | 15 |
| 8.1 Princípios do Novo GEIT | 16 |
| 8.2 Foco Crescente nos Facilitadores | 16 |
| 8.3 Novo Modelo de Referência de Processos | 16 |
| 8.4 Processos novos e modificados separando Governança de Gestão..... | 17 |
| 8.5 Práticas e Atividades | 17 |
| 8.6 Metas e Métricas Melhoradas | 17 |
| 8.7 Entradas e Saídas revisadas e melhoradas..... | 17 |
| 8.8 Gráficos RACI expandidos..... | 17 |
| 8.9 Novo Modelo de Maturidade de Capacidade de Processo..... | 18 |
| 9. REFERÊNCIAS | 18 |
| APÊNDICE A – OBJETIVOS EM CASCATA..... | 20 |
| APÊNDICE B – DOMÍNIOS E PROCESSOS DO COBIT 5 | 22 |
| APÊNDICE C – DESCRIÇÃO DO PROCESSO BAI06: GERENCIAR MUDANÇAS | 27 |

Lista de Figuras

| | |
|--|----|
| Figura 1 – Os Cinco Princípios do COBIT 5..... | 6 |
| Figura 2 – Criação de Valor..... | 7 |
| Figura 3 – Visão Geral dos Objetivos em Cascata..... | 8 |
| Figura 4 – Abordagem de Governança..... | 9 |
| Figura 5 – Os Sete Facilitadores do COBIT 5 | 10 |
| Figura 6 – O Modelo Geral dos Facilitadores..... | 11 |
| Figura 7 – Áreas Chaves da Governança e da Gestão..... | 12 |
| Figura 8 – Modelo de Referência de Processos (PRM) do Domínio Governança e os 37 processos | 13 |
| Figura 9 – As sete fases de implementação do ciclo de vida | 14 |
| Figura 10 – Modelo de Capacidade de Processos Genérico | 15 |
| Figura 11 – COBIT 5: Integração de Frameworks do ISACA | 16 |
| Figura 12 – Gráficos RACI COBIT 4.1 e COBIT 5 | 18 |
| Figura 13 – Metas Empresariais | 20 |
| Figura 14 – Metas de TI Relacionadas | 21 |

Manual de Treinamento Pré-Curso do COBIT® 5 Foundation



Obrigado por adquirir nosso Treinamento do COBIT® 5. O objetivo principal deste guia é fornecer um conteúdo fácil de ler e fácil de entender. As ideias para este guia vieram das perguntas que recebemos das pessoas tentando aprender

COBIT® 5 e o fato de que o Manual Oficial do COBIT® 5 é uma excelente referência, mas não é um Manual de Treinamento. O Manual Oficial do COBIT® 5 pode ser um pouco difícil de usar e ler se você é novo em Governança de TI. Você aproveitará mais o Manual Oficial, se primeiro entender as informações contidas neste Manual de Treinamento. Doravante, este guia pretende ser (e, é) uma preparação (antecipada) para seu curso COBIT® 5 Foundation, de forma que você poderá chegar ao treinamento de fato mais preparado, e se baseia no *syllabus* do Exame *Foundation*.

Feedback: Agradecemos por seu retorno (correções ou sugestões de melhoria)

E-mail para contato@mpplaza.com.br

COBIT® is a trademark of ISACA® registered in the United States and other countries.

Cursos COBIT® 5 – Presencial / e-Learning

MP Esse Material de Treinamento é Aprovado pela **APMG-International**

MP Este Manual de Treinamento fará parte de nosso treinamento COBIT®5 Foundation

Agradecimentos:

Tradução : Ernani Marques

Revisão Final da Tradução/Diagramação : Ronielton Oliveira

Direitos de Distribuição [Copyright]

Com exceção a pequenas passagens e situações, nenhuma parte dessa publicação pode ser reproduzida ou transmitida de qualquer maneira, ou por qualquer meio, sem o prévio consentimento. Claro, agradecemos sugestões. Este manual foi fornecido a você com a condição de que ele não seja copiado, modificado, publicado, vendido, *rebranded*, alugado, ou distribuído para fins comerciais.

Sobre Management Plaza Brasil



A Management Plaza Brasil é especializada em Governança de TI e Melhores Práticas em Gerenciamento de Projetos.

A visão do ATO é tonar-se um provedor acreditado global de todas os produtos oferecidos pelo Grupo APMG ao ser uma empresa referência em treinamentos de metodologias e melhores práticas.

Nossa missão é prover Capacitação de Qualidade, contribuindo para o diferencial competitivo das organizações e dos profissionais.

É o Melhor conteúdo da Europa disponível por um preço justo e disponível a VOCÊ!

E-mail: contato@mpplaza.com.br

Website: www.managementplaza.com.br

O nosso Instrutor Lider Ernani Marques é Certificado em COBIT® 4.1 – Foundation COBIT® 5 – Foundation e COBIT® 5 – **Implementação**. Conosco, você tem os melhores materiais e os melhores treinamentos.

1. Introdução

A quinta versão do COBIT foi lançada em abril de 2012, e sua ênfase está em alinhar à realidade da TI e das organizações. Essa versão traz mudanças na estrutura de processos e introduz novos conceitos. Alguns assuntos não contemplados pelo COBIT 4.1 e que são discutidos em Governança agora estão inseridos no contexto do COBIT 5.

O COBIT 5 é a integração de conceitos e princípios do COBIT 4.1 com outros *frameworks* do *Information Systems Audit and Control Association* (ISACA®), tais como: Val IT, Risk IT, BMIS e ITAF. Além disso, alinhama-se a outros padrões de mercado como ITIL®, ISO®, Guia PMBOK®, TOGAF® e PRINCE2®. Sem dúvidas, está nova versão ajuda as empresas a criar valor para TI, mantendo o equilíbrio entre os investimentos em recursos e os riscos organizacionais, uma vez que consideram os negócios, as áreas funcionais de TI da empresa e as partes interessadas, tanto internas como externas.

2. Novidades do COBIT 5

O COBIT 5 tem foco em Governança Corporativa de TI, muito bem delimitando **a relação existente entre Governança e Gestão**. Provê um *framework* que auxilia as corporações a atingirem suas metas e sustentam-nas a entregar valor por meio de uma efetiva governança e gestão da TI empresarial.

É baseado em 5 princípios que permitem que a organização construa um *framework* efetivo de governança e gerenciamento de TI suportado por um conjunto holístico de 7 facilitadores que aperfeiçoam os investimentos em tecnologia e informação utilizados para o benefício das partes interessadas.

3. Princípios

O *framework* baseia-se em 5 princípios:



Figura 1 – Os Cinco Princípios do COBIT 5

3.1 Atender as necessidades das partes interessadas

As organizações existem para criar valor para as partes interessadas. Para cada parte interessada, a criação de valor pode representar interesses diferentes e algumas vezes conflitantes. A governança tem a função de negociar e decidir entre os diferentes interesses destas partes interessadas. O sistema de

governança deve considerar a opinião de todos os envolvidos quando são tomadas as decisões sobre os benefícios, recursos e avaliação dos riscos. A Figura 2, ilustra os objetivos das partes interessadas. Sempre, para cada decisão de governança, as seguintes perguntas devem ser feitas:

- Quem recebe os benefícios?
- Quem suporta os riscos?
- Quais são os recursos necessários?

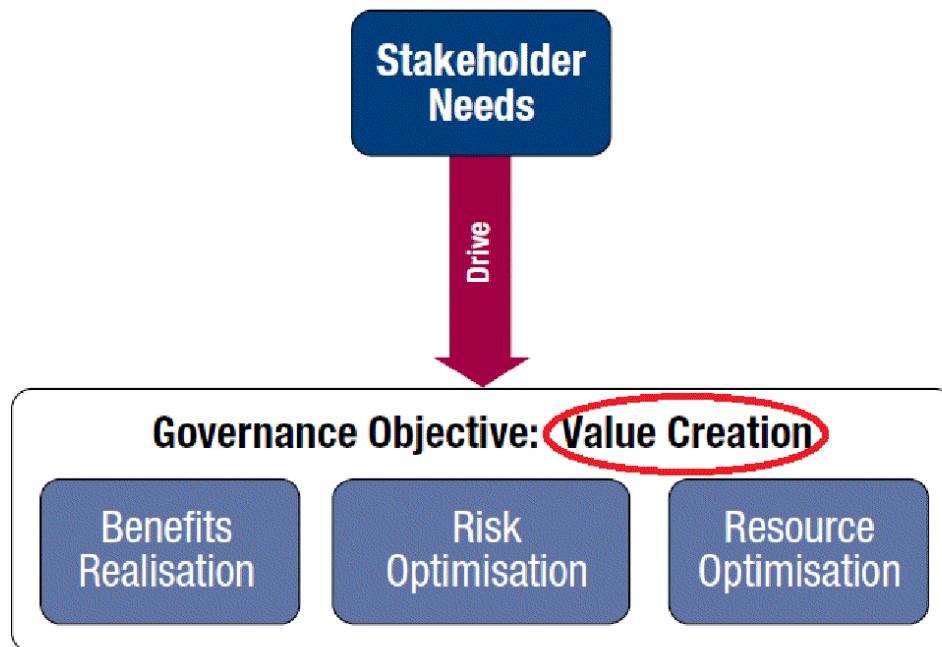


Figura 2 – Criação de Valor

Fonte: (ISACA, 2012a, p. 17)

As necessidades das partes interessadas precisam ser transformadas em estratégias corporativas. Para isso, há o mecanismo **Objetivos em Cascata**, que tem por finalidade, desdobrar:

- As necessidades das partes interessadas em Metas Empresariais;
- As Metas Empresariais em Metas de TI;
- As Metas de TI em Metas de Facilitadores.

A Figura 3, ilustra o funcionamento do mecanismo Objetivos em Cascata. Note que elas derivam de cima para baixo. E, para que haja um bom alinhamento, o ideal é que você consiga efetuar a leitura e ligação das metas de cima para baixo (*top-down*) e de baixo para cima (*bottom-up*).

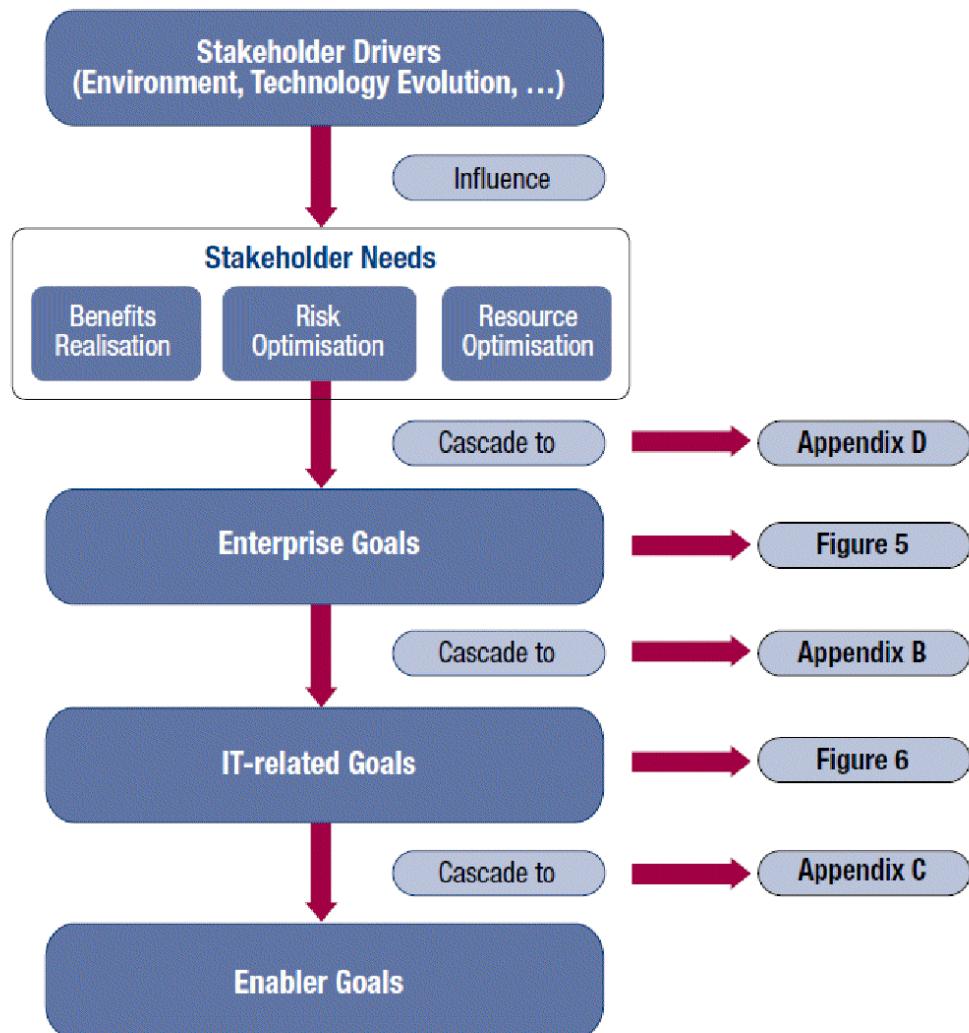


Figura 3 – Visão Geral dos Objetivos em Cascata

Fonte: (ISACA, 2012a, p. 18)

3.2 Abranger a empresa de ponta-a-ponta

O COBIT 5 trata a governança e gerenciamento de TI cobrindo a organização de ponta a ponta. Isso significa:

- Integra a governança de TI empresarial dentro da governança;
- Cobre todas as funções e processos requeridos dentro da organização;
- Não foca apenas nas funções de TI, mas abrange a informação e tecnologia relacionadas como ativos que precisam ser tratados como qualquer outro ativo por todos na organização.
- Abordagem de Governança, proposta pelo COBIT 5 pode ser visualizada na Figura 4.

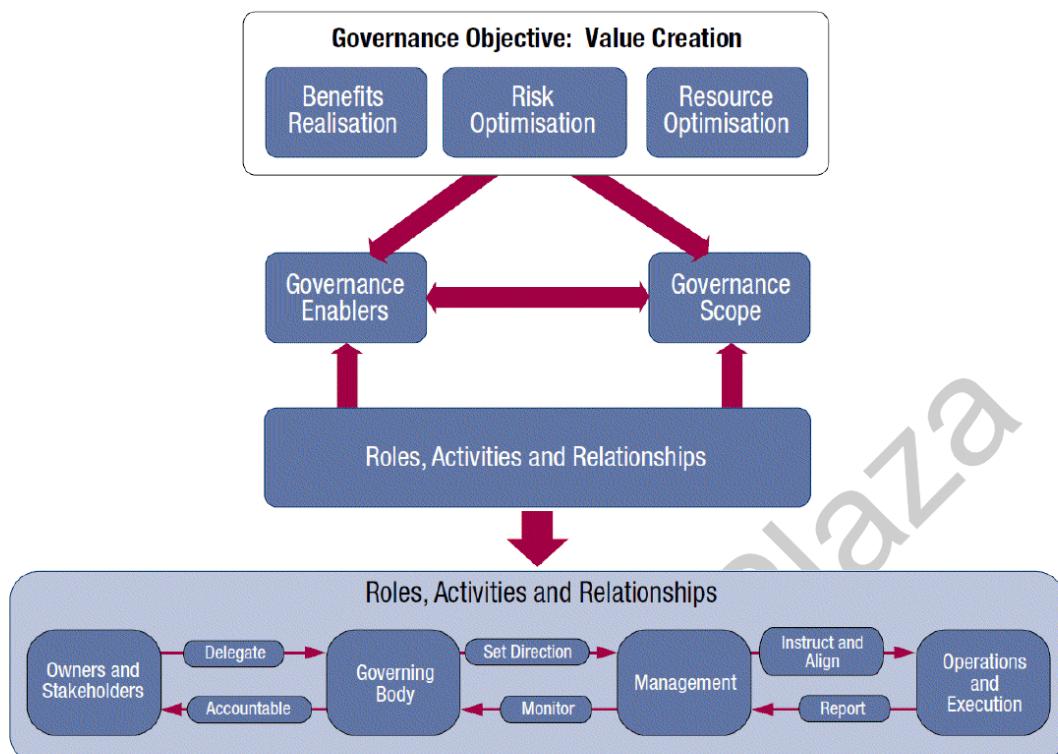


Figura 4 – Abordagem de Governança

Fonte: (ISACA, 2012a, p. 23, 24)

Além dos objetivos de governança, os outros componentes da abordagem são:

- **Facilitadores da Governança:** são os recursos organizacionais usados na governança como princípios, estruturas, processos e práticas.
- **Escopo da Governança:** área em que será aplicada a governança (toda a organização ou só uma parte).
- **Regras, Atividades e Relacionamentos:** define quem está envolvido com governança, como estarão envolvidos, o que farão e como irão interagir dentro do escopo da governança.

3.3 Aplicar um *framework* único e integrado

O COBIT 5 está alinhado com os mais atuais e relevantes padrões e *frameworks* utilizados nas corporações, com: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000; e também com os relacionados a TI: ISO/IEC 38500, ITIL, ISO/IEC 27000 series, TOGAF; e ao gerenciamento de projetos, Guia PMBOK®, Gerenciando Projetos de Sucesso com PRINCE2®, CMMI, etc. De fato, isto permite à organização utilizar o COBIT 5 como um integrador dos *frameworks* de governança e de gestão.

3.4 Facilitar uma abordagem holística

Para que haja uma governança e gestão de TI empresarial, eficientes e eficazes é necessário uma abordagem holística, levando em conta vários componentes que interagem entre si. O COBIT 5 define um conjunto de **facilitadores** que suportam a implementação de um sistema de governança e gerenciamento de TI. Estes, são fatores que, individual e coletivamente, influenciam o funcionamento da governança e gestão corporativa. São classificados em 7 categorias:

1. **Princípios, Políticas e Estruturas:** são os veículos que traduzem o comportamento desejado em um guia prático para a gestão cotidiana.
2. **Processos:** descrevem um conjunto organizado de práticas e atividades para atingir certos objetivos e produzir um conjunto de saídas que auxiliem no cumprimento das metas relacionadas a TI.

3. **Estruturas Organizacionais:** são as entidades-chave, responsáveis pela tomada de decisão em uma organização.
 4. **Cultura, Ética e Comportamento:** dos indivíduos e da organização; muito frequentemente é subestimada como um fator de sucesso nas atividades de governança e gestão.
 5. **Informação:** está difundida por toda organização. Representa todas as informações produzidas e utilizadas pela organização. Informação é requerida para manter a organização em funcionamento e bem governada.
 6. **Serviços, Infraestrutura e Aplicações:** inclui a infraestrutura, tecnologia e as aplicações que fornecem à organização os serviços e processamento de TI.
 7. **Pessoas, Habilidades e Competências:** está relacionado com as pessoas e são requeridas para que as atividades sejam executadas com sucesso e para que decisões e ações corretivas sejam realizadas de forma correta.

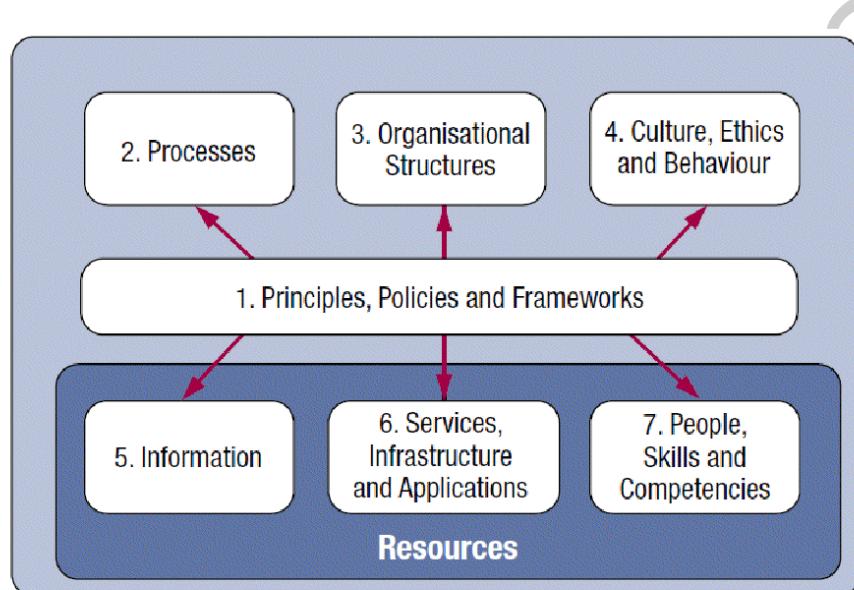


Figura 5 – Os Sete Facilitadores do COBIT 5

Fonte: (ISACA, 2012a, p. 27)

3.4.1 Dimensões de Facilitadores

Todos os facilitadores têm um conjunto de dimensões comuns:

- Fornece uma maneira comum, simples e estruturada para lidar com facilitadores;
 - Permite que uma entidade gerencie suas interações complexas;
 - Facilita a resultados bem sucedidos dos facilitadores.

As quatro dimensões para os facilitadores, que estão ilustradas na Figura 6, são:

- **Partes interessadas:** cada facilitador tem partes que desempenham um papel ativo e/ ou têm interesse na execução. Por exemplo, os processos têm diferentes partes que executam atividades de processo e/ou que têm interesse no resultado do processo; estruturas organizacionais têm partes, cada uma com seus próprios papéis e interesses, que fazem parte da estrutura. As partes interessadas podem ser internas ou externas à empresa, todos com seus interesses e necessidades.
 - **Metas:** cada facilitador tem uma série de objetivos e fornece valor pela realização destes objetivos. As metas podem ser definidas em termos de:
 - Resultados esperados do facilitador.
 - Aplicação ou operação do próprio facilitador.
 - **Ciclo de Vida:** cada facilitador tem um ciclo de vida, ou seja, é definido, criado, operado, monitorado, atualizado e descontinuado. As fases do ciclo de vida consistem em:

- Planejar (inclui o desenvolvimento de conceitos e seleção de conceitos).
- Projetar.
- Construir/adquirir/criar/implementar.
- Utilizar/operar.
- Avaliar/monitorar.
- Atualizar/eliminar.
- **Boas Práticas:** para cada um dos facilitadores, boas práticas podem ser definidas. Boas práticas apoiam a realização dos objetivos do facilitador. Boas práticas fornecem exemplos ou sugestões sobre a melhor forma de implementar o facilitador, e quais os produtos de trabalho, entradas e saídas são requeridos.

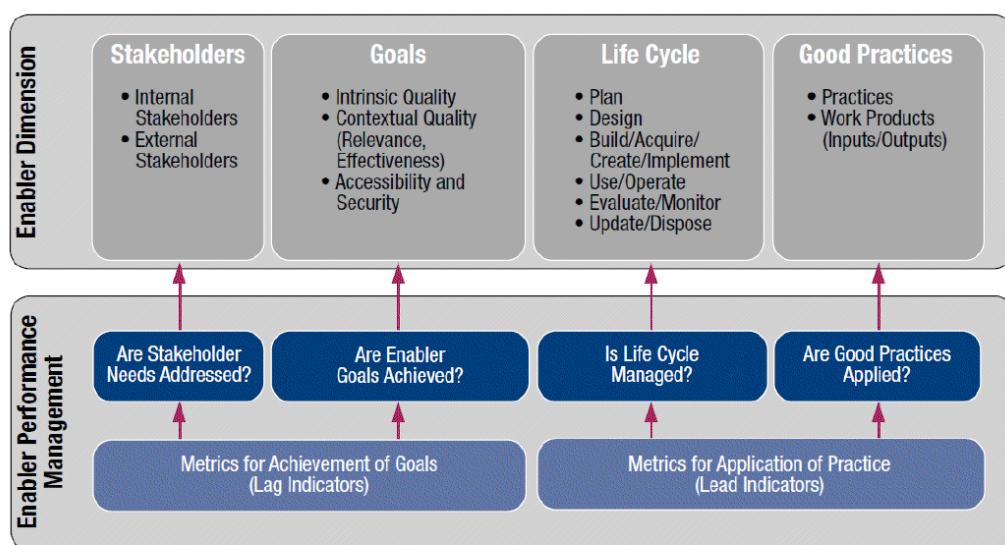


Figura 6 – O Modelo Geral dos Facilitadores

Fonte: (ISACA, 2012a, p. 28)

3.5 Separar a Governança da Gestão

O COBIT 5 torna clara a distinção entre governança e gestão. Essas duas disciplinas abrangem diferentes tipos de atividades, exigem diferentes estruturas organizacionais e servem a propósitos diferentes.

A governança assegura que as necessidades das partes interessadas, as condições e as opções sejam avaliadas para determinar os objetivos de negócios a serem alcançados; define a direção por meio de priorização e tomada de decisão; e monitoramento de desempenho e conformidade com relação aos objetivos. Na maioria das organizações, a governança é de responsabilidade do Conselho Diretor, sob a liderança do presidente. Responsabilidades de governança específicas podem ser delegadas a estruturas organizacionais especiais em um nível apropriado, especialmente em empresas maiores e complexas.

A gestão planeja, constrói, executa e monitora atividades alinhadas com a direção dada pela governança para alcançar os objetivos de negócios. Na maioria das empresas, a gestão é da responsabilidade da gerência executiva, sob a liderança do chefe executivo (CEO).

4. Novo Modelo de Referência de Processos

O novo Modelo de Referência de Processos do COBIT 5 subdivide os processos de TI em duas principais áreas de atuação – Governança e Gestão – e, estes contêm processos agrupados em domínios, conforme Figura 7

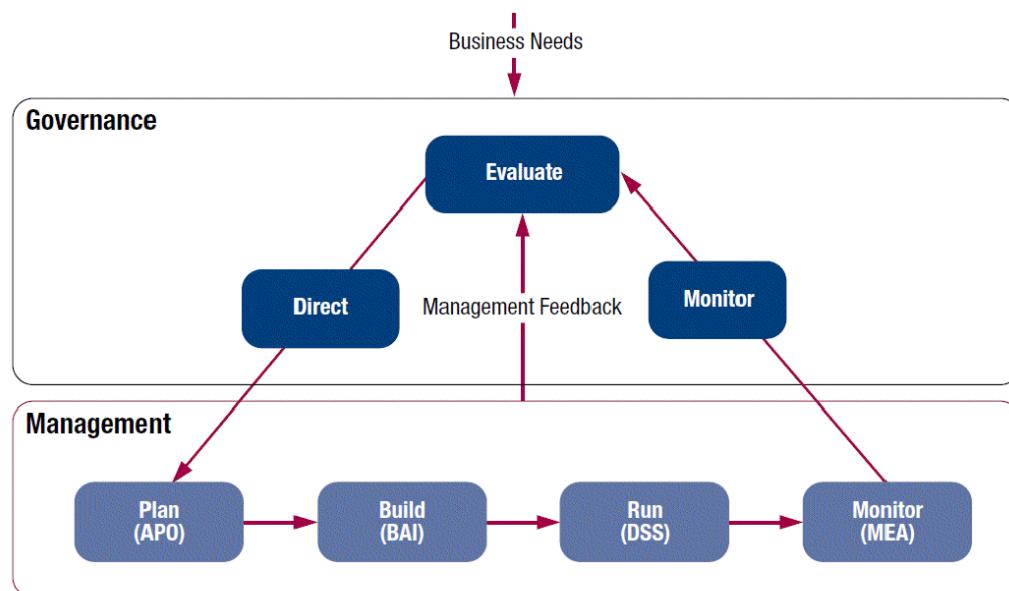


Figura 7 – Áreas Chaves da Governança e da Gestão

Fonte: (ISACA, 2012a, p. 32)

Esses domínios agrupam os processos por sinergia e no âmbito da Governança os processos estão mais associados a efetuar direcionamentos, e também a propiciar a tomada de decisão para novos direcionamentos. Por outro lado, no domínio da Gestão, os processos estão relacionados ao planejamento e condução de ações mais táticas.

Como estes dois grandes domínios precisam manter o sincronismo, é de fundamental importância que organização adote abordagens estratégicas, como por exemplo: *Management of Portfolios* (MoP)® e *Managing a Successful Programs* (MSP)® em conjunto com abordagens mais táticas que também funcionem em sintonia, como por exemplo, Gerenciamento de Projetos de Sucesso com PRINCE2® com as abordagens estratégicas.

4.1 Processos de Governança

Contém um domínio **Avaliar, Dirigir e Monitorar (EDM)** com 5 processos de governança. Dentro de cada processo, são definidas práticas de avaliar, dirigir e monitorar.

4.2 Processos de Gerenciamento

Contém 4 domínios, de acordo com as áreas de responsabilidade de planejar, criar, executar e monitorar (PBRM) e oferece cobertura ponta-a-ponta de TI. Estes domínios são uma evolução da estrutura de domínios e processos do COBIT 4.1. Os domínios são:

- **Alinhar, Planejar e Organizar (APO)**
- **Construir, Adquirir e Implementar (BAI)**
- **Entrega, Serviço e Suporte (DSS)**
- **Monitorar, Analisar e Avaliar (MEA)**

A Figura 8 exibe os 37 processos de governança e gerenciamento do COBIT 5. Os detalhes de cada processo estão no manual *COBIT 5: Enabling Processes*. No *COBIT 5: Enabling Processes*, cada um dos 37 processos são desdobrados em práticas de governança ou práticas de gerenciamento. Essas práticas de governança e de gerenciamento são equivalentes aos objetivos de controle do COBIT 4.1, práticas de gerenciamento do Val IT e do Risk IT. O Apêndice B, relaciona todos os processos com a respectiva descrição.

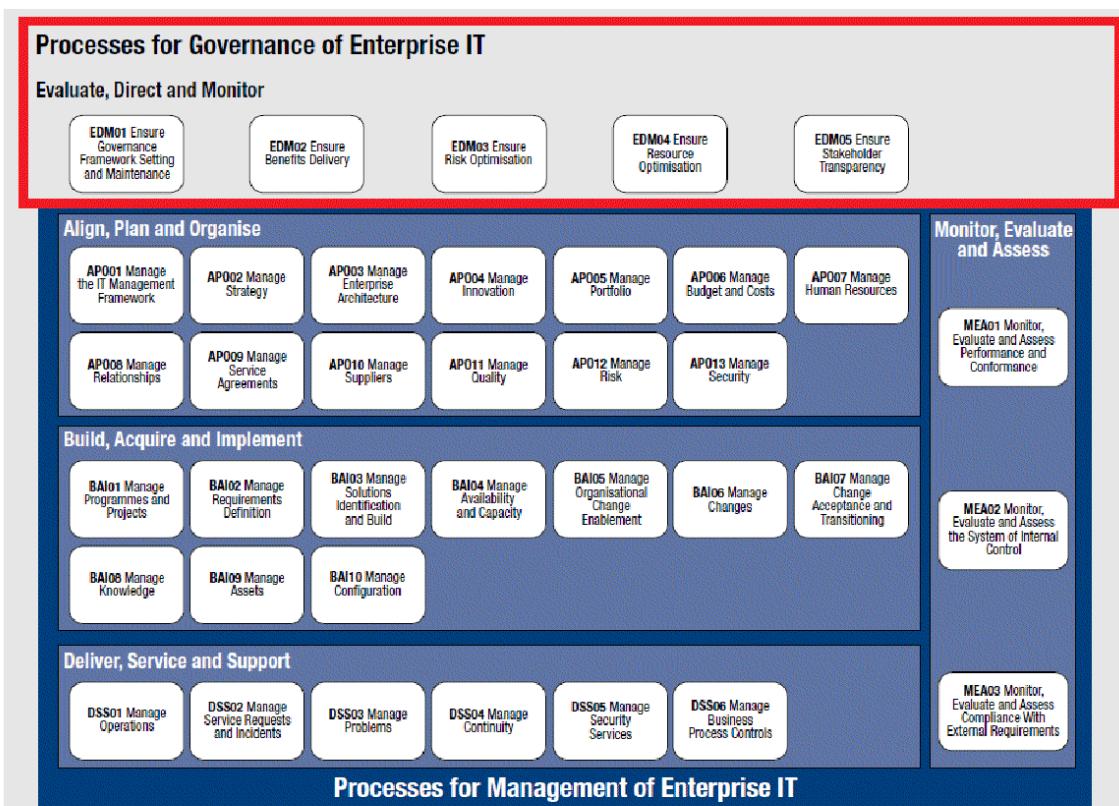


Figura 8 – Modelo de Referência de Processos (PRM) do Domínio Governança e os 37 processos

Fonte: (ISACA, 2012a, p. 33)

5. Estrutura de Processos

Para cada processo, as seguintes informações são incluídas, de acordo com o modelo de processo:

- Identificação do processo:
 - Rótulo do Processo: o domínio (EDM, APO, BAI, DSS, MEA) e o número do processo;
 - Nome do Processo: breve descrição do processo; e,
 - Área do processo: governança ou de gestão.
 - Nome do domínio
- Descrição – uma visão do que o processo faz e como o processo alcança seu propósito.
- Propósito do Processo – descrição geral do propósito do processo.
- Informação dos objetivos em cascata – referência e descrição dos objetivos relacionados com a TI que são essencialmente suportados pelo processo e métricas para medir o alcance dos objetivos relacionados com a TI.
- Objetivos de processos e métricas – um conjunto de metas de processo e um número limitado de exemplo de métricas.
- Matriz RACI – uma sugestão de atribuição de nível de responsabilidade por práticas de processos para diferentes funções e estruturas.
- Descrição detalhada de práticas de processo para cada prática:
 - Título da Prática e descrição;
 - Entradas e saídas da prática, com indicação de origem e destino; e,
 - As atividades de processo, detalhando ainda mais as práticas.
- Guias relacionados – associa cada processo do COBIT a outros frameworks que podem ser usados para implementar o processo.

O Apêndice C contém a descrição do processo BAI06: Gerenciar Mudanças.

6. Ciclo de Vida da Implementação

O ciclo de vida de implementação é uma forma das organizações usarem o COBIT 5 para lidar com a complexidade e desafios encontrados normalmente durante as implementações. Existem três componentes inter-relacionados neste ciclo de vida:

- Melhoria contínua (núcleo).
- Habilitação de mudança (2º anel).
- Gerenciamento do programa (3º anel).

O ciclo de vida e as suas 7 fases estão ilustrados na Figura 9.

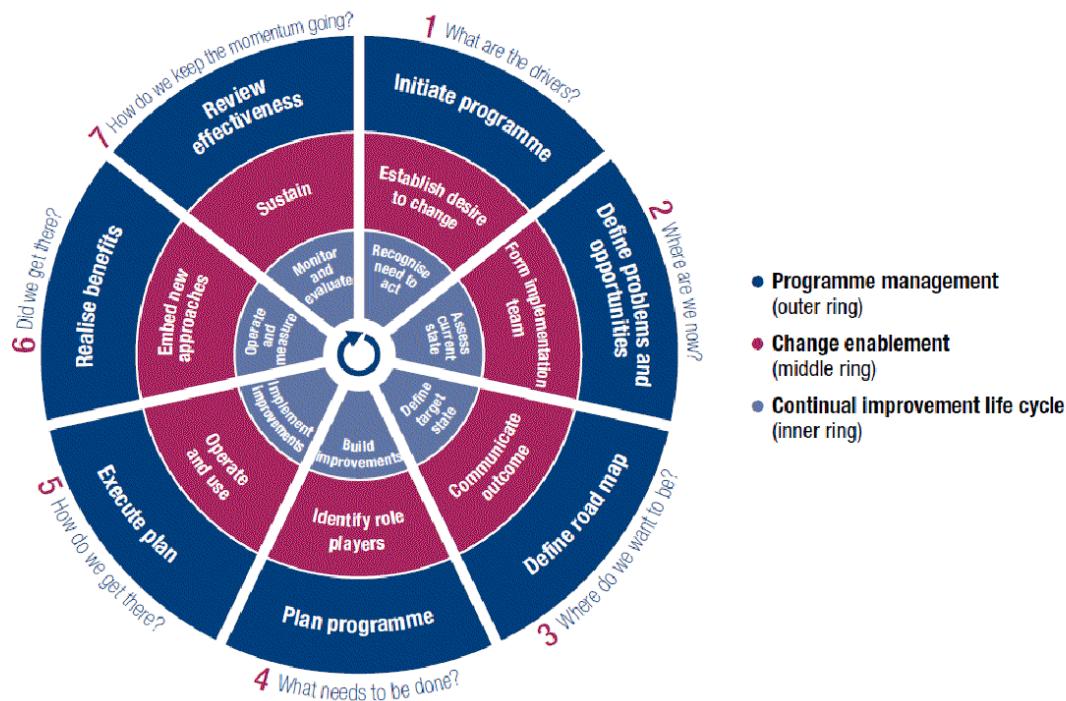


Figura 9 – As sete fases de implementação do ciclo de vida

Fonte: (ISACA, 2012a, p. 37)

- **Fase 1:** começa com o reconhecimento e concordância da necessidade de governar TI.
- **Fase 2:** está focada em definir o escopo da iniciativa de implementação ou melhoria.
- **Fase 3:** uma meta de melhoria é definida e seguida por uma análise mais detalhada.
- **Fase 4:** planeja soluções práticas através da definição de projetos apoiados por casos de negócios justificáveis.
- **Fase 5:** as soluções propostas são implementadas nas práticas do dia-a-dia.
- **Fase 6:** incide sobre a operação sustentável dos facilitadores novos ou melhorados e o monitoramento da realização dos benefícios esperados.
- **Fase 7:** o sucesso global da iniciativa é revista.

7. Modelo de Capacidade de Processos

O COBIT 5 traz um novo modelo para a avaliação da capacidade dos processos de TI da organização baseado na norma ISO/IEC 15504. O modelo de capacidade de processos do COBIT 5 é exibido na Figura 10.

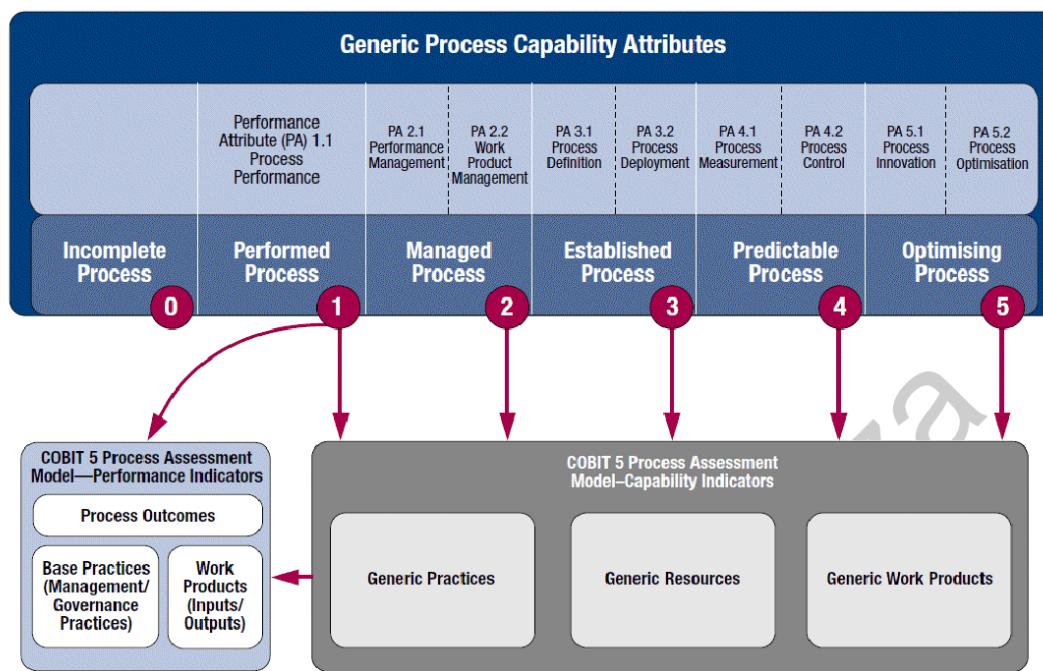


Figura 10 – Modelo de Capacidade de Processos Genérico

Fonte: (ISACA, 2012a, p. 42)

Existem seis níveis de capacidade que um processo pode alcançar, incluindo a designação de um “processo incompleto” se as práticas nele não alcançam o efeito pretendido do processo:

- **Processo Incompleto:** o processo não está implementado ou não atinge seu objetivo. Nesse nível, há pouca ou nenhuma evidência de realização sistemática da finalidade do processo.
- **Processo Realizado** (um atributo): possui o atributo “Desempenho do Processo”.
- **Processo Gerenciado** (dois atributos): possui os atributos “Gestão do Desempenho” e “Gestão do Produto do Trabalho”.
- **Processo Estabelecido** (dois atributos): possui os atributos “Definição do Processo” e “Implementação do Processo”.
- **Processo Previsível** (dois atributos): possui os atributos “Medição do Processo” e “Controle do Processo”.
- **Processo Otimizado** (dois atributos): possui os atributos “Inovação do Processo” e “Otimização do Processo”.

Cada nível de capacidade só pode ser alcançado quando o nível inferior for totalmente alcançado. Por exemplo, uma capacidade de processo nível 3 (Processo Estabelecido), exige que os atributos Definição do Processo e Implementação do Processo sejam alcançados SOBRE a plena realização dos atributos para um nível de capacidade do processo 2 (Processo Gerenciado).

8. Resumo das Diferenças COBIT 4.1 e COBIT 5

Os usuários do COBIT 4.1, Val IT e Risk IT já envolvidos em atividades de implementação da Governança de TI Empresarial (GEIT) podem migrar para o COBIT 5 e beneficiar-se com as orientações melhoradas e mais recentes. O COBIT 5 foi construído sobre as versões do COBIT 4.1, Val IT e Risk IT, então, a empresa pode dar continuidade a partir do que já foi desenvolvido com o apoio das versões anteriores.

A seguir as maiores mudanças do conteúdo do COBIT 5 e como elas podem impactar a implementação/melhoria do GEIT:

1. Novos Princípios GEIT
2. Foco crescente nos facilitadores
3. Novo Modelo de Referência de Processos
4. Processos novos e modificados separando Governança de Gestão

5. Práticas e Atividades
6. Metas e Métricas revisadas e expandidas
7. Entradas e Saídas revisadas e melhoradas
8. Gráficos RACI expandidos no nível de prática de gestão
9. Novo Modelo de Maturidade de Capacidade de Processo

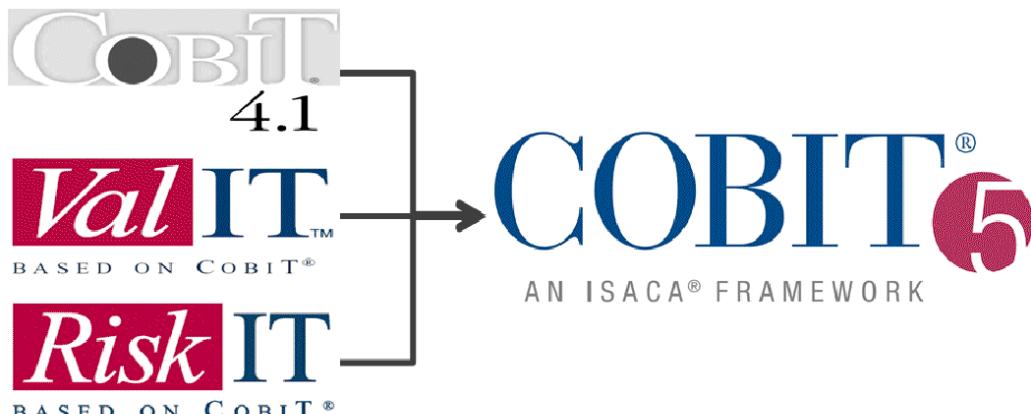


Figura 11 – COBIT 5: Integração de Frameworks do ISACA

8.1 Princípios do Novo GEIT

Os frameworks Val IT e Risk IT são baseados em princípios. O *feedback* indica que os princípios são fáceis de entender e de serem aplicados no contexto empresarial, permitindo que o valor derive do guia de suporte mais eficazmente. A ISO/IEC 38500 também incorpora princípios para sustentar suas mensagens para atingir a distribuição de lucro do mesmo mercado, embora os princípios deste padrão e do COBIT5 não sejam os mesmos.

8.2 Foco Crescente nos Facilitadores

- O COBIT 4.1 não possuía facilitadores? Sim, tinha, porém não eram chamados facilitadores.
- Informação, Infraestrutura e Aplicações (serviços) e pessoas (Pessoas, Habilidades e Competências) eram os recursos do COBIT 4.1.
 - Princípios, Políticas e Estruturas foram mencionados em alguns processos do COBIT 4.1.
 - Processos eram centrais ao uso do COBIT 4.1.
 - A Estrutura Organizacional estava implícita através das funções RACI e suas definições.
 - Cultura, Ética e Comportamento eram mencionados em alguns processos do COBIT 4.1.

8.3 Novo Modelo de Referência de Processos

O COBIT 5 se baseia em um Modelo de Referência de Processos revisado com um novo domínio de governança e vários processos novos e modificados que agora abrangem atividades ponta-a-ponta – por exemplo, negócios e áreas de funcionais de TI.

O COBIT 5 consolida o COBIT 4.1, Val IT e Risk IT em único *framework*, e tem sido atualizado para alinhar-se às melhores práticas correntes, por exemplo, ITIL e TOGAF. O novo modelo pode ser utilizado enquanto um guia para ajustar quando necessário o próprio modelo de processo empresarial (como o COBIT 4.1).

Quadro 1 – Comparativo de Processos entre COBIT 4.1 e COBIT 5

| COBIT 4.1 | COBIT 5 |
|---|--|
| - | EDM (Avaliar, Dirigir e Monitorar) 5 processos |
| PO (Planejar e Organizar) 10 processos | APO (Alinhar, Organizar e Planejar) 13 processos |
| AI (Adquirir e Implementar) 7 processos | BAI (Construir, Adquirir e Implementar) 10 processos |

| | |
|---|---|
| DS (Entregar e Suportar) 13 processos | DSS (Entrega, Serviço e Suporte) 6 processos |
| ME (Monitorar e Avaliar) 4 processos | MEA (Monitorar, Analisar e Avaliar) 3 processos |

OBSERVAÇÃO: O COBIT 4.1 tinha 34 processos. O COBIT 5 tem 37 divididos em Governança e Gestão.

8.4 Processos novos e modificados separando Governança de Gestão

O COBIT 5 apresenta cinco novos processos de governança que tem capacitado e melhorado as abordagens de governança do COBIT 4.1, Val IT e Risk IT. Esta orientação:

- Ajuda as empresas para mais tarde refinar e fortalecer práticas e atividades do nível GEIT da gestão executiva.
- Apoia a integração do GEIT com práticas de governança empresariais existentes e se alinha com a ISO/IEC 38500.

Há vários processos novos e modificados que refletem o pensamento corrente, em particular:

- APO03 Gerenciar a arquitetura corporativa.
- APO04 Gerenciar a inovação.
- APO05 Gerenciar o portfólio.
- APO06 Gerenciar o orçamento e custos.
- APO08 Gerenciar os relacionamentos.
- APO13 Gerenciar a segurança.
- BAI05 Gerenciar a implementação de mudança organizacional.
- BAI08 Gerenciar o conhecimento.
- BAI09 Gerenciar os ativos.
- DSS05 Gerenciar os serviços de segurança.
- DSS06 Gerenciar os controles de processos de negócio.

Os processos do COBIT 5 agora abrangem negócios ponta-a-ponta, e atividades de TI, por exemplo, uma visão em nível corporativo. Este fornece uma abrangência mais holística e completa de práticas que refletem a ampla natureza invasiva empresarial quanto ao uso da TI. Isto torna o envolvimento, as responsabilidades e as obrigações das partes interessadas dos negócios mais explícitos e transparentes.

8.5 Práticas e Atividades

A governança e as práticas de gestão do COBIT 5 são equivalentes aos objetivos de controle do COBIT 4.1 e processos do Val IT e Risk IT. O COBIT 5 integra e atualiza todo o conteúdo prévio num único modelo, facilitando aos usuários a compreensão e utilização deste material na implementação de melhorias.

8.6 Metas e Métricas Melhoradas

O COBIT 5 segue os mesmos conceitos de meta e métrica do COBIT 4.1, Val IT e Risk IT, mas estes são renomeados: Metas Empresariais, Metas de TI e Metas de Facilitadores, refletindo uma visão em nível corporativo.

O COBIT 5 fornece o mecanismo de Objetivos em Cascata, que traduz a concepção das metas por meio de uma cascata revisada baseada nas Metas Empresariais direcionando as Metas de TI e então, apoiando os processos críticos, conforme descrito no Apêndice A.

O COBIT 5 fornece exemplos de metas e métricas nos níveis de prática de gestão e processo empresarial. Isto é uma mudança do COBIT 4.1, Val IT e Risk IT, os quais desceram um nível.

8.7 Entradas e Saídas revisadas e melhoradas

O COBIT 5 fornece entradas e saídas para cada prática de gestão, enquanto o COBIT 4.1 apenas as fornecia em nível de processo. Então, o COBIT 5 fornece orientação detalhada adicional para o desenho de processos para a inclusão de produtos de trabalho essenciais e assistência com a integração entre processos.

8.8 Gráficos RACI expandidos

No COBIT 4.1, os gráficos RACI se encontravam apenas em Nível de Processo. No COBIT 5, está no nível de Prática de Gestão, conforme mostrado na Figura 12.

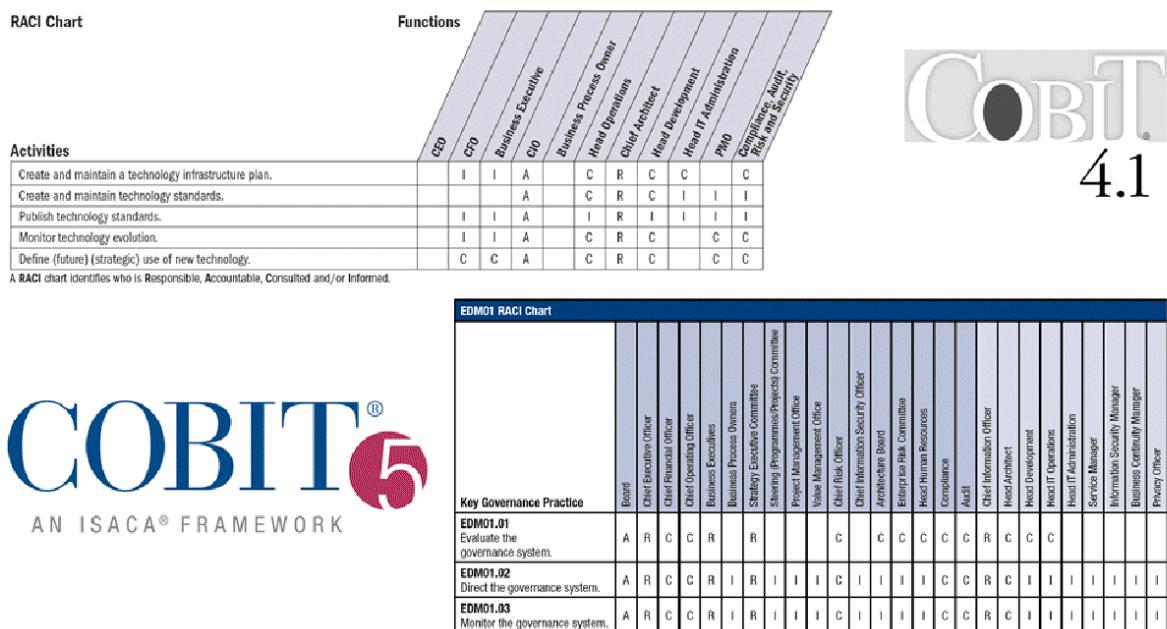


Figura 12 – Gráficos RACI COBIT 4.1 e COBIT 5

Fonte: (ISACA, 2012a) e (ITGI, 2007)

8.9 Novo Modelo de Maturidade de Capacidade de Processo

O COBIT 5 interrompe a abordagem do Modelo de Maturidade de Capacidade baseado em CMM do COBIT4.1, Val IT e Risk IT. O COBIT 5 é apoiado por uma nova abordagem de avaliação de capacidade de processo baseada na ISO/IEC 15504, e o Programa de Avaliação do COBIT tem sido estabelecido para o COBIT 4.1 como uma alternativa à abordagem CMM.

As abordagens com base em CMM do COBIT4.1, Val IT e Risk IT, não são consideradas compatíveis com a abordagem ISO/EIC 15504 porque os métodos usam atributos e escalas de mensuração diferentes. Então, a abordagem do Programa de Avaliação do COBIT é considerada pelo ISACA como mais robusta, confiável e repetitiva enquanto um método de avaliação de capacidade de processo.

O Programa de Avaliação do COBIT apoia:

- Avaliações formais por assessores acreditados.
- Auto avaliações menos rigorosas para análise de insuficiências internas e planejamento de melhoria de processo.
- No futuro, o Programa de Avaliação do COBIT, também capacitará potencialmente uma empresa para obter valores certificados e independentes alinhados ao padrão ISO/IEC.
- Usuários do COBIT 4.1, Val IT e Risk IT que desejem passar para a abordagem do novo Programa de Avaliação do COBIT precisarão realinear suas avaliações anteriores, adotar e aprender o novo método, e iniciar um novo conjunto de valores de modo a ganhar os benefícios da nova abordagem.
- Embora algumas informações reunidas a partir das avaliações anteriores possam ser reutilizáveis, será necessário o cuidado na migração das mesmas, pois há diferenças significativas nos requisitos.

9. Referências

DOURADO, L. Apostila COBIT 5. **Tecnologia da Informação e Comunicações(TIC)& Concurso Público**, 22 out. 2013. Disponível em: <<http://lmdourado.wordpress.com/2013/10/22/apostila-cobit-5/>>. Acesso em: 21 fev. 2014.

ISACA. **COBIT 5**: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, Illinois: Information Systems Audit and Control Association, 2012a. 94 p. Download disponível em <http://www.isaca.org/COBIT/Pages/Product-Family.aspx>.

ISACA. **COBIT 5**: Enabling Processes. Rolling Meadows, Illinois: Information Systems Audit and Control Association, 2012b. 230 p. Download disponível em <http://www.isaca.org/COBIT/Pages/Product-Family.aspx>.

ITGI. **COBIT 4.1**: Framework Control Objectives Management Guidelines Maturity Models. Rolling Meadows, IL: IT Governance Institute, 2007. 213 p. Download disponível em <http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx>.

Management Plaza

Apêndice A – Objetivos em Cascata

A Figura 3 apresentou o mecanismo Objetivos em Cascata, o qual tem a finalidade de desdobrar:

- As necessidades das partes interessadas em Metas Empresariais;
- As Metas Empresariais em Metas de TI;
- As Metas de TI em Metas de Facilitadores.

Esse desdobramento é descrito em quatro passos:

Passo 1: Diretrizes das Partes Interessadas influenciam as necessidades das Partes Interessadas

As necessidades das partes interessadas são influenciadas por um número de diretrizes, por exemplo, mudanças na estratégia, mudança no ambiente de negócios, mudanças nas leis vigentes e novas tecnologias.

Passo 2: Necessidades das Partes Interessadas desdobrados em Objetivos de Negócio

As necessidades das Partes Interessadas podem ser relacionadas a um conjunto de objetivos de negócio genéricos. Esses objetivos podem ser desenvolvidos usando as dimensões do *Balanced Score Card* (BSC) e representam uma lista de objetivos comumente usados por uma organização. Embora essa lista não seja exaustiva, a maioria dos objetivos específicos de uma organização pode ser mapeada para um ou mais objetivos de negócio genéricos.

COBIT 5 define 17 Metas Empresariais genéricas, como mostrado na Figura 13, que incluem as seguintes informações:

- A dimensão BSC ao qual o objetivo pertence;
- Objetivos de negócio;
- O relacionamento dos três objetivos principais de governança – Realização de Benefícios, Otimização de Risco e Otimização de Recursos ('P' indica relacionamento primário e 'S' relacionamento secundário).

| BSC Dimension | Enterprise Goal | Relation to Governance Objectives | | |
|---------------------|---|-----------------------------------|-------------------|-----------------------|
| | | Benefits Realisation | Risk Optimisation | Resource Optimisation |
| Financial | 1. Stakeholder value of business investments | P | | S |
| | 2. Portfolio of competitive products and services | P | P | S |
| | 3. Managed business risk (safeguarding of assets) | | P | S |
| | 4. Compliance with external laws and regulations | | P | |
| | 5. Financial transparency | P | S | S |
| Customer | 6. Customer-oriented service culture | P | | S |
| | 7. Business service continuity and availability | | P | |
| | 8. Agile responses to a changing business environment | P | | S |
| | 9. Information-based strategic decision making | P | P | P |
| | 10. Optimisation of service delivery costs | P | | P |
| Internal | 11. Optimisation of business process functionality | P | | P |
| | 12. Optimisation of business process costs | P | | P |
| | 13. Managed business change programmes | P | P | S |
| | 14. Operational and staff productivity | P | | P |
| | 15. Compliance with internal policies | | P | |
| Learning and Growth | 16. Skilled and motivated people | S | P | P |
| | 17. Product and business innovation culture | P | | |

Figura 13 – Metas Empresariais

Fonte: (ISACA, 2012a, p. 19)

Passo 3: Metas Empresariais desdobradas em metas de TI

O alcance dos objetivos de negócio exige uma série de resultados relacionados a TI, que são representados pelos objetivos relacionados a TI. O COBIT 5 define 17 Metas de TI Relacionadas, as quais são exibidas na Figura 14

| IT BSC Dimension | Information and Related Technology Goal | |
|---------------------|---|---|
| Financial | 01 | Alignment of IT and business strategy |
| | 02 | IT compliance and support for business compliance with external laws and regulations |
| | 03 | Commitment of executive management for making IT-related decisions |
| | 04 | Managed IT-related business risk |
| | 05 | Realised benefits from IT-enabled investments and services portfolio |
| | 06 | Transparency of IT costs, benefits and risk |
| Customer | 07 | Delivery of IT services in line with business requirements |
| | 08 | Adequate use of applications, information and technology solutions |
| Internal | 09 | IT agility |
| | 10 | Security of information, processing infrastructure and applications |
| | 11 | Optimisation of IT assets, resources and capabilities |
| | 12 | Enablement and support of business processes by integrating applications and technology into business processes |
| | 13 | Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards |
| | 14 | Availability of reliable and useful information for decision making |
| Learning and Growth | 15 | IT compliance with internal policies |
| | 16 | Competent and motivated business and IT personnel |
| | 17 | Knowledge, expertise and initiatives for business innovation |

Figura 14 – Metas de TI Relacionadas

Fonte: (ISACA, 2012a, p. 19)

Passo 4: Metas de TI desdobradas em Metas de Facilitadores

Alcançar as Metas de TI Relacionadas requer a aplicação e uso bem-sucedidos de um conjunto de facilitadores. Facilitadores incluem:

- Princípios, Políticas e Estruturas
- Processos
- Estruturas Organizacionais
- Cultura, Ética e Comportamento
- Informação
- Serviços, Infraestrutura e Aplicações
- Pessoas, Habilidades e Competências

Para cada facilitador, um conjunto de objetivos específicos e relevantes pode ser definido em apoio aos objetivos relacionados a TI. Os objetivos do processo são fornecidos nas descrições detalhadas do processo.

Apêndice B – Domínios e Processos do COBIT 5

| EDM (Avaliar, Dirigir e Monitorar) | | |
|------------------------------------|--|--|
| EDM01 | Assegurar o estabelecimento e a manutenção do <i>framework</i> de governança | Analisa e articula os requisitos para a governança corporativa de TI, coloca em prática e mantém estruturas, princípios, processos e práticas, com clareza de responsabilidades e autoridade para alcançar a missão, as metas e os objetivos da organização. |
| EDM02 | Assegurar a entrega de benefícios | Otimiza 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. |
| EDM03 | Assegurar a otimização de riscos | Assegura que o apetite e tolerância a riscos da organização são compreendidos, articulados e comunicados e que o risco ao valor da organização relacionado ao uso de TI é identificado e controlado. |
| EDM04 | Assegurar a otimização de recursos | Assegura que as capacidades adequadas e suficientes relacionadas a TI (pessoas, processos e tecnologia) estão disponíveis para apoiar os objetivos da organização de forma eficaz a um custo ótimo. |
| EDM05 | Assegurar a transparência para as partes interessadas | Assegura que a medição e relatórios de desempenho e conformidade da TI corporativa sejam transparentes para as partes interessadas aprovarem as metas, métricas e as ações corretivas necessárias. |

| APO (Alinhar, Organizar e Planejar) | | |
|-------------------------------------|--|--|
| APO01 | Gerenciar o <i>framework</i> de gestão de TI | Esclarece e mantém a missão e visão da governança de TI da organização. Implementa e mantém mecanismos e autoridades para gerenciar a informação e o uso da TI na organização. |
| APO02 | Gerenciar a estratégia | Fornece uma visão holística do negócio e ambiente de TI atual, a direção futura, e as iniciativas necessárias para migrar para o ambiente futuro desejado. |
| APO03 | Gerenciar a arquitetura corporativa | Estabelece uma arquitetura comum que consiste em processos de negócios, informações, dados, aplicação e tecnologia para realizar de forma eficaz e eficiente as estratégias de negócio e de TI por meio da criação de modelos e práticas-chave que descrevem arquitetura de linha de base. |

| | | |
|-------|---------------------------------|---|
| APO04 | Gerenciar a inovação | Mantém uma consciência de TI e tendências de serviços relacionados, identifica oportunidades de inovação e planeja como se beneficiar da inovação em relação às necessidades do negócio. Influencia o planejamento estratégico e as decisões de arquitetura corporativa. |
| APO05 | Gerenciar o portfólio | Executa o conjunto de orientações estratégicas para os investimentos alinhados com a visão de arquitetura corporativa e as características desejadas do investimento e considerar as restrições de recursos e de orçamento. Avalia, prioriza programas e serviços, gerencia demanda dentro das restrições de recursos e de orçamento, com base no seu alinhamento com os objetivos estratégicos e risco. Move programas selecionados para o portfólio de serviços para execução. Monitora o desempenho de todo o portfólio de serviços e programas, propondo os ajustes necessários em resposta ao programa e desempenho do serviço ou mudança de prioridades da organização. |
| APO06 | Gerenciar o orçamento e custos | Administrar as atividades financeiras relacionadas a TI tanta nas funções de negócios e de TI, abrangendo orçamento, gerenciamento de custos e benefícios e priorização dos gastos com o uso de práticas formais de orçamento e de um sistema justo e equitativo de alocação de custos para a organização. |
| APO07 | Gerenciar recursos humanos | Fornecer uma abordagem estruturada para garantir a estruturação ideal, colocação, direitos de decisão e as habilidades dos recursos humanos. Isso inclui a comunicação de papéis e responsabilidades definidas, planos de aprendizagem e de crescimento, e as expectativas de desempenho, com o apoio de pessoas competentes e motivadas. |
| APO08 | Gerenciar os relacionamentos | Gerencia o relacionamento entre o negócio e TI de uma maneira formal e transparente, que garanta foco na realização de um objetivo comum. |
| APO09 | Gerenciar os acordos de serviço | Alinha serviços de TI e níveis de serviço com as necessidades e expectativas da organização, incluindo identificação, especificação, projeto, publicação, acordo, e acompanhamento de serviços de TI, níveis de serviço e indicadores de desempenho. |
| APO10 | Gerenciar os fornecedores | Gerencia serviços relacionados a TI prestados por todos os tipos de fornecedores para atender às necessidades organizacionais, incluindo a seleção de fornecedores, gestão de relacionamentos, gestão de contratos e revisão e monitoramento de desempenho de fornecedores para a efetividade e conformidade. |
| APO11 | Gerenciar a qualidade | Define e comunica os requisitos de qualidade em todos os processos, os procedimentos e os resultados das organizações, incluindo controles, monitoramento contínuo, e o uso de práticas comprovadas e padrões na melhoria contínua e esforços de eficiência. |

| | | |
|-------|-----------------------|---|
| APO12 | Gerenciar os riscos | Identificar continuamente, avaliar e reduzir os riscos relacionados a TI dentro dos níveis de tolerância estabelecidos pela diretoria executiva da organização. |
| APO13 | Gerenciar a segurança | Define, opera e monitora um sistema para a gestão de segurança da informação. |

| BAI (Construir, Adquirir e Implementar) | | |
|--|---|--|
| BAI01 | Gerenciar programas e projetos | Gerenciar todos os programas e projetos do portfólio de investimentos em alinhamento com a estratégia da organização e de forma coordenada. Inicia, planeja, controla e executa programas e projetos, e finaliza com uma revisão pós-implementação. |
| BAI02 | Gerenciar a definição de requisitos | Identifica soluções e analisa os requisitos antes da aquisição ou criação para assegurar que eles estão em conformidade com os requisitos estratégicos corporativos que cobrem os processos de negócio, aplicações, informações/ dados, infraestrutura e serviços. Coordena com as partes interessadas afetadas a revisão de opções viáveis, incluindo custos e benefícios, análise de risco e aprovação de requisitos e soluções propostas. |
| BAI03 | Gerenciar a identificação e construção de soluções | Estabelece e mantém soluções identificadas em conformidade com os requisitos da organização abrangendo design, desenvolvimento, aquisição/terceirização e parcerias com fornecedores/vendedores. Gerencia configuração, teste de preparação, testes, requisitos de gestão e manutenção dos processos de negócio, aplicações, informações/dados, infraestrutura e serviços. |
| BAI04 | Gerenciar a disponibilidade e capacidade | Equilibra as necessidades atuais e futuras de disponibilidade, desempenho e capacidade de prestação de serviços de baixo custo. Inclui a avaliação de capacidades atuais, a previsão das necessidades futuras com base em requisitos de negócios, análise de impactos nos negócios e avaliação de risco para planejar e implementar ações para atender as necessidades identificadas. |
| BAI05 | Gerenciar a implementação de mudança organizacional | Maximiza a probabilidade de implementar com sucesso a mudança organizacional sustentável em toda a organização de forma rápida e com risco reduzido, cobrindo o ciclo de vida completo da mudança e todas as partes interessadas afetadas no negócio e TI. |
| BAI06 | Gerenciar mudanças | Gerencia todas as mudanças de uma maneira controlada, incluindo mudanças de padrão e de manutenção de emergência relacionadas com os processos de negócio, aplicações e infraestrutura. Isto inclui os padrões de mudança e procedimentos, avaliação de impacto, priorização e autorização, mudanças emergenciais, acompanhamento, elaboração de relatórios, encerramento e documentação. |

| | | |
|-------|---|---|
| BAI07 | Gerenciar aceite e transição de mudança | Aceita e produz formalmente novas soluções operacionais, incluindo planejamento de implementação do sistema, e conversão de dados, testes de aceitação, comunicação, preparação de liberação, promoção para produção de processos de negócios e serviços de TI novos ou alterados, suporte de produção e uma revisão pós-implementação. |
| BAI08 | Gerenciar o conhecimento | Mantém a disponibilidade de conhecimento relevante, atual, validado e confiável para suportar todas as atividades do processo e facilitar a tomada de decisão. Plano para a identificação, coleta, organização, manutenção, utilização e retirada de conhecimento. |
| BAI09 | Gerenciar os ativos | Gerencia os ativos de TI através de seu ciclo de vida para assegurar que seu uso agraga valor a um custo ideal. Os ativos permanecem operacionais e fisicamente protegidos e aqueles que são fundamentais para apoiar a capacidade de serviço são confiáveis e disponíveis. |
| BAI10 | Gerenciar a configuração | Define e mantém as descrições e as relações entre os principais recursos e as capacidades necessárias para prestar serviços de TI, incluindo a coleta de informações de configuração, o estabelecimento de linhas de base, verificação e auditoria de informações de configuração e atualizar o repositório de configuração. |

| DSS (Entrega, Serviço e Suporte) | | |
|----------------------------------|---|---|
| DSS01 | Gerenciar as operações | Coordena e executa as atividades e procedimentos operacionais necessários para entregar serviços de TI internos e terceirizados, incluindo a execução de procedimentos operacionais, padrões pré-definidos e as atividades exigidas. |
| DSS02 | Gerenciar requisições de serviço e incidentes | Fornece uma resposta rápida e eficaz às solicitações dos usuários e resolução de todos os tipos de incidentes. Restaurar o serviço normal; recorda e atender às solicitações dos usuários e registro, investigar, diagnosticar, escalar e solucionar incidentes. |
| DSS03 | Gerenciar problemas | Identifica e classifica os problemas e suas causas-raízes e fornece resolução para prevenir incidentes recorrentes. Fornece recomendações de melhorias. |
| DSS04 | Gerenciar a continuidade | Estabelece e mantém um plano para permitir o negócio e TI responder a incidentes e interrupções, a fim de continuar a operação de processos críticos de negócios e serviços de TI necessários e mantém a disponibilidade de informações em um nível aceitável para a organização. |

| | | |
|-------|--|---|
| DSS05 | Gerenciar os serviços de segurança | Protege informações da organização para manter o nível de risco aceitável para a segurança da informação da organização, de acordo com a política de segurança. Estabelece e mantém as funções de segurança da informação e privilégios de acesso e realiza o monitoramento de segurança. |
| DSS06 | Gerenciar os controles de processos de negócio | Define e mantém controles de processo de negócio apropriados para assegurar que as informações relacionadas e processadas satisfazem todos os requisitos de controle de informações relevantes. |

| MEA (Monitorar, Analisar e Avaliar) | | |
|-------------------------------------|--|---|
| MEA01 | Monitorar, analisar e avaliar o desempenho e conformidade | Coleta, valida e avalia os objetivos e métricas do processo de negócios e de TI. Monitora se os processos estão realizando conforme metas e métricas de desempenho e conformidade acordadas e fornece informação que é sistemática e oportuna. |
| MEA02 | Monitorar, analisar e avaliar o sistema de controle interno | Monitora e avalia continuamente o ambiente de controle, incluindo auto avaliações e análises de avaliações independentes. Permite o gerenciamento de identificar deficiências de controle e ineficiências e iniciar ações de melhoria. |
| MEA03 | Monitorar, analisar e avaliar a Conformidade com requisitos externos | Avalia se processos de TI e processos de negócios suportados pela TI estão em conformidade com as leis, regulamentos e exigências contratuais. Obtém a garantia de que os requisitos foram identificados e respeitados, e integra-os à conformidade com o conhecimento global da organização. |

Apêndice C – Descrição do Processo BAI06: Gerenciar Mudanças

| BAI06 Manage Changes | | Area: Management Domain: Build, Acquire and Implement |
|---|--|--|
| Process Description Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation. | | |
| Process Purpose Statement Enable fast and reliable delivery of change to the business and mitigation of the risk of negatively impacting the stability or integrity of the changed environment. | | |
| The process supports the achievement of a set of primary IT-related goals: | | |
| IT-related Goal | | Related Metrics |
| 04 Managed IT-related business risk | | <ul style="list-style-type: none"> Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment Number of significant IT-related incidents that were not identified in risk assessment Percent of enterprise risk assessments including IT-related risk Frequency of update of risk profile |
| 07 Delivery of IT services in line with business requirements | | <ul style="list-style-type: none"> Number of business disruptions due to IT service incidents Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels Percent of users satisfied with the quality of IT service delivery |
| 10 Security of information, processing infrastructure and applications | | <ul style="list-style-type: none"> Number of security incidents causing financial loss, business disruption or public embarrassment Number of IT services with outstanding security requirements Time to grant, change and remove access privileges, compared to agreed-on service levels Frequency of security assessment against latest standards and guidelines |
| Process Goals and Metrics | | |
| Process Goal | | Related Metrics |
| 1. Authorised changes are made in a timely manner and with minimal errors. | | <ul style="list-style-type: none"> Amount of rework caused by failed changes Reduced time and effort required to make changes Number and age of backlogged change requests |
| 2. Impact assessments reveal the effect of the change on all affected components. | | <ul style="list-style-type: none"> Percent of unsuccessful changes due to inadequate impact assessments |
| 3. All emergency changes are reviewed and authorised after the change. | | <ul style="list-style-type: none"> Percent of total changes that are emergency fixes Number of emergency changes not authorised after the change |
| 4. Key stakeholders are kept informed of all aspects of the change. | | <ul style="list-style-type: none"> Stakeholder feedback ratings on satisfaction with communications |

| BAI06 RACI Chart | | Board | Chief Executive Officer | Chief Financial Officer | Chief Operating Officer | Business Executives | Business Process Owners | Strategy Executive Committee | Steering (Programmes/Projects) Committee | Project Management Office | Value Management Office | Chief Risk Officer | Chief Information Security Officer | Architecture Board | Enterprise Risk Committee | Head Human Resources | Compliance | Audit | Chief Information Officer | Head Architect | Head Development | Head IT Operations | Head IT Administration | Service Manager | Information Security Manager | Business Continuity Manager | Privacy Officer | |
|-------------------------|----------|-------|-------------------------|-------------------------|-------------------------|---------------------|-------------------------|------------------------------|--|---------------------------|-------------------------|--------------------|------------------------------------|--------------------|---------------------------|----------------------|------------|-------|---------------------------|----------------|------------------|--------------------|------------------------|-----------------|------------------------------|-----------------------------|-----------------|---|
| Key Management Practice | BAI06.01 | | | | A | R | | C | C | | | | C | C | R | C | R | R | C | R | C | R | C | I | R | R | I | C |
| BAI06.02 | | | | | A | I | | C | | | | | C | C | R | I | R | R | | I | C | | | | | | | |
| BAI06.03 | | | | | C | R | | C | | | | | | | | A | R | R | | R | | R | | | | | | |
| BAI06.04 | | | | | A | R | | R | C | | | | C | C | R | C | R | R | I | I | | | | | | | | |

(ISACA, 2012b)

| BAI06 Process Practices, Inputs/Outputs and Activities | | | | | | |
|--|----------|---|---|----------|--|--|
| Management Practice | Inputs | | Outputs | | | |
| | From | Description | Description | To | | |
| BAI06.01 Evaluate, prioritise and authorise change requests. Evaluate all requests for change to determine the impact on business processes and IT services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritised, categorised, assessed, authorised, planned and scheduled. | BAI03.05 | Integrated and configured solution components | Impact assessments | Internal | | |
| | DSS02.03 | Approved service requests | Approved requests for change | BAI07.01 | | |
| | DSS03.03 | Proposed solutions to known errors | | | | |
| | DSS03.05 | Identified sustainable solutions | Change plan and schedule | BAI07.01 | | |
| | DSS04.08 | Approved changes to the plans | | | | |
| | DSS06.01 | Root cause analyses and recommendations | | | | |
| Activities | | | | | | |
| 1. Use formal change requests to enable business process owners and IT to request changes to business process, infrastructure, systems or applications. Make sure that all such changes arise only through the change request management process. | | | | | | |
| 2. Categorise all requested changes (e.g., business process, infrastructure, operating systems, networks, application systems, purchased/packaged application software) and relate affected configuration items. | | | | | | |
| 3. Prioritise all requested changes based on the business and technical requirements, resources required, and the legal, regulatory and contractual reasons for the requested change. | | | | | | |
| 4. Plan and evaluate all requests in a structured fashion. Include an impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified. Assess the likelihood of adversely affecting the operational environment and the risk of implementing the change. Consider security, legal, contractual and compliance implications of the requested change. Consider also inter-dependencies amongst changes. Involve business process owners in the assessment process, as appropriate. | | | | | | |
| 5. Formally approve each change by business process owners, service managers and IT technical stakeholders, as appropriate. Changes that are low-risk and relatively frequent should be pre-approved as standard changes. | | | | | | |
| 6. Plan and schedule all approved changes. | | | | | | |
| 7. Consider the impact of contracted services providers (e.g., of outsourced business processing, infrastructure, application development and shared services) on the change management process, including integration of organisational change management processes with change management processes of service providers and the impact on contractual terms and SLAs. | | | | | | |
| Management Practice | Inputs | | Outputs | | | |
| BAI06.02 Manage emergency changes. Carefully manage emergency changes to minimise further incidents and make sure the change is controlled and takes place securely. Verify that emergency changes are appropriately assessed and authorised after the change. | From | Description | Description | To | | |
| | | | Post-implementation review of emergency changes | Internal | | |
| Activities | | | | | | |
| 1. Ensure that a documented procedure exists to declare, assess, give preliminary approval, authorise after the change and record an emergency change. | | | | | | |
| 2. Verify that all emergency access arrangements for changes are appropriately authorised, documented and revoked after the change has been applied. | | | | | | |
| 3. Monitor all emergency changes, and conduct post-implementation reviews involving all concerned parties. The review should consider and initiate corrective actions based on root causes such as problems with business process, application system development and maintenance, development and test environments, documentation and manuals, and data integrity. | | | | | | |
| 4. Define what constitutes an emergency change. | | | | | | |

Fonte: (ISACA, 2012b)

-X- FIM -X-