MODELO COBIT

MISSÃO DO COBIT:
Pesquisar, desenvolver, publicar e promover um modelo de controle para governança de TI atualizado e internacionalmente reconhecido para ser adotado por organizações e utilizado no dia-a-dia por gerentes de negócios, profissionais de TI e profissionais de avaliação.

A NECESSIDADE DE UM MODELO DE CONTROLE PARA A GOVERNANÇA DE TI

Um modelo de controle da governança de TI define as razões pelas quais a governança de TI é necessária, quais são as partes interessadas e o que esse modelo precisa atingir.

Por quê

Cada vez mais a Alta Direção está percebendo o significativo impacto que a informação tem no sucesso da organização. Os executivos esperam um alto entendimento sobre a forma como TI funciona e o quanto ela está sendo bem administrada para atingir vantagens competitivas. Em particular, os executivos precisam saber se as informações estão sendo gerenciadas pela empresa de modo a:
- Possivelmente atingir os objetivos
- Ter resiliência suficiente para aprender e se adaptar
- Gerenciar adequadamente os riscos encontrados
- Apropriadamente reconhecer as oportunidades e agir sobre elas

As organizações não podem atingir seus requisitos de negócios e governança sem adotar e implementar um modelo para governança e controle de TI para:
- Fazer uma ligação com os requisitos de negócios
- Tornar transparente a performance obtida comparada a esses requisitos
- Organizar as atividades de acordo com um modelo de processos geralmente aceito
- Identificar os recursos mais importantes a serem aprimorados
- Definir os objetivos de controles gerenciais a serem considerados

Adicionalmente, as metodologias de governança e controle estão tornando-se parte das boas práticas de gerenciamento de TI e são facilitadoras para o estabelecimento de governança de TI e aderência aos cada vez mais crescentes requisitos regulatórios.

As boas práticas de TI tornaram-se significantes devido a inúmeros fatores:
- Executivos de negócio e a Alta Direção demandando um melhor retorno dos investimentos em TI, isto é, que a área de TI entregue as necessidades da área de negócios para aumentar o valor para partes interessadas
- Preocupação com o aumento observado dos gastos com TI
- A necessidade de atender às exigências regulatórias de controles de TI em áreas como privacidade de informações e relatórios financeiros (por exemplo, Lei Sarbanes-Oxley e Basiléia II) e regulamentações para setores específicos como as áreas de finanças, farmacêutica e saúde
- Seleção de provedores de serviços e o gerenciamento e aquisição de serviços terceirizados
- Os riscos relacionados a TI cada vez mais complexos, como a segurança de redes
- Iniciativas de governança de TI que incluem a adoção de metodologias de controles e boas práticas que ajudem a monitorar e aprimorar as atividades críticas de TI para ampliar o valor do negócio e reduzir os riscos.
- A necessidade de otimizar os custos seguindo, sempre que possível, um enfoque padronizado em vez de abordagens especialmente desenvolvidas.
- A crescente maturidade e consequente aceitação de metodologias bem-sucedidas, tais como o COBIT, IT Infrastructure Library (ITIL), séries ISO 27000 sobre padrões relacionados à segurança da informação, ISO 9001:2000 – Requerimentos – Sistemas de Gerenciamento de Qualidade, Capability Maturity Model Integration (CMNI), Projects in Controlled Environments 2 (PRINCE2) e o Guide to the Project Management Body of Knowledge (PMBOK).
- A necessidade de as empresas avaliarem como estão em relação aos padrões geralmente aceitos e em comparação seus parceiros e organizações similares *(benchmarking)*

Quem

Uma metodologia de governança e controles precisa servir a uma variedade de partes interessadas tanto internas como externas, cada uma com necessidades especificas:

- Partes interessadas dentro da empresa *(stakeholders)* que procuram gerar valor a partir dos investimentos em TI:
  - Aqueles que tomam decisões sobre investimentos
  - Aqueles que decidem sobre requisitos
  - Aqueles que usam os serviços de TI
- Partes interessadas dentro e fora da empresa que fornecem serviços de TI:
  - Aqueles que gerenciam a organização e os processos de TI
  - Aqueles que desenvolvem as capacidades
  - Aqueles que operam os serviços
- Partes interessadas dentro e fora da empresa que têm responsabilidades sobre controles/riscos:
  - Aqueles com responsabilidades sobre segurança, confidencialidade e/ou riscos
  - Aqueles que executam funções de conformidade
  - Aqueles que requerem ou fornecem serviços de avaliação

O quê

Para atender aos requisitos listados na seção anterior, uma metodologia de governança e controle de TI deve:

- Fornecer um foco de negócios para permitir o alinhamento entre os objetivos de negócios e de TI
- Estabelecer um processo de orientação para definir os escopos e a extensão da cobertura, com uma estrutura definida permitindo uma fácil navegação em seu conteúdo
- Ser geralmente aceita por ser consistente com as boas práticas e padrões de TI e independente de tecnologias específicas
- Prover uma linguagem comum com um conjunto de termos e definições geralmente entendidos por todas as partes interessadas
- Ajudar a atender aos requisitos regulatórios por ser consistente com padrões de governança geralmente aceitos (como o COSO) e controles de TI esperados por reguladores e auditores externos

COMO O CobiT ATENDE A NECESSIDADE

Em respostas às necessidades descritas na seção anterior, o modelo CobiT foi criado com as principais características de ser focado em negócios, orientado a processos, baseado em controles e orientado por medições.

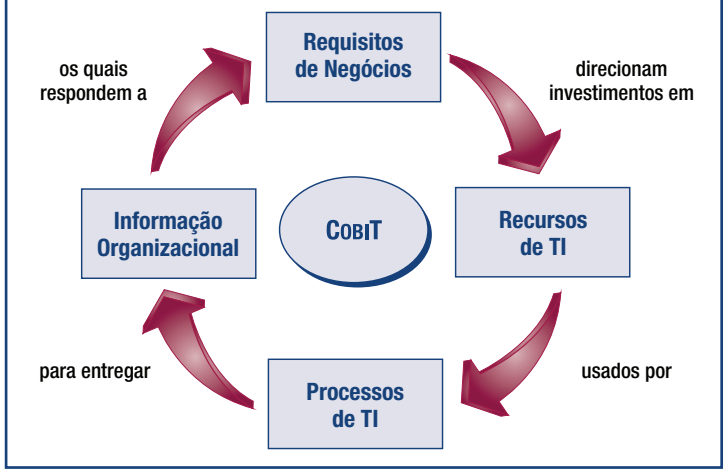
Focado em negócios

A orientação para negócios é o principal tema do CobiT, o qual foi desenvolvido não somente para ser utilizado por provedores de serviços, usuários e auditores, mas também, e mais importante, para fornecer um guia abrangente para os executivos e donos de processos de negócios.

O modelo CobiT é baseado nos seguintes princípios (figura 5): Prover a informação de que a organização precisa para atingir os seus objetivos, as necessidades para investir, gerenciar e controlar os recursos de TI usando um conjunto estruturado de processos para prover os serviços que disponibilizam as informações necessárias para a organização.

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

Figura 5 - Princípios Básicos do CobiT



CRITÉRIOS DE INFORMAÇAO DO CobiT

Para atender aos objetivos de negócios, as informações precisam se adequar a certos critérios de controles, aos quais o CobiT denomina necessidades de informação da empresa. Baseado em abrangentes requisitos de qualidade, guarda e segurança, sete critérios de informação distintos e sobrepostos são definidos, como segue:

- **Efetividade** lida com a informação relevante e pertinente para o processo de negócio bem como a mesma sendo entregue em tempo, de maneira correta, consistente e utilizável.
- **Eficiência** relaciona-se com a entrega da informação através do melhor (mais produtivo e econômico) uso dos recursos.
- **Confidencialidade** está relacionada com a proteção de informações confidenciais para evitar a divulgação indevida.

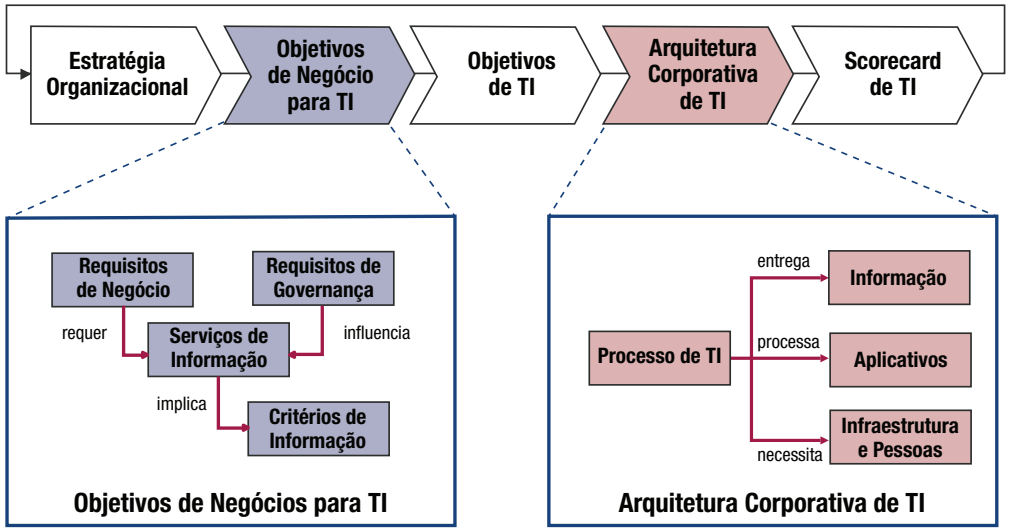
- **Integridade** relaciona-se com a fidedignidade e totalidade da informação bem como sua validade de acordo os valores de negócios e expectativas.
- **Disponibilidade** relaciona-se com a disponibilidade da informação quando exigida pelo processo de negócio hoje e no futuro. Também está ligada à salvaguarda dos recursos necessários e capacidades associadas.
- **Conformidade** lida com a aderência a leis, regulamentos e obrigações contratuais aos quais os processos de negócios estão sujeitos, isto é, critérios de negócios impostos externamente e políticas internas.
- **Confiabilidade** relaciona-se com a entrega da informação apropriada para os executivos para administrar a entidade e exercer suas responsabilidades fiduciárias e de governança.

OBJETIVOS DE NEGÓCIOS E OBJETIVOS DE TI

Enquanto os critérios de informação fornecem um método genérico para definir os requisitos de negócios, definir um conjunto genérico de objetivos de negócios e de TI fornece uma base mais refinada para o estabelecimento dos requisitos de negócios e o desenvolvimento de métricas que permitam avaliar se esses objetivos foram atendidos. Toda organização usa TI para fazer funcionar as iniciativas de negócios e essas podem ser representadas como objetivos de negócios para a área de TI. Esses exemplos genéricos podem ser utilizados como um guia para determinar os requisitos de negócios específicos, as metas e as métricas para a organização.

Para a área de TI entregar de maneira bem-sucedida os serviços que suportam as estratégias de negócios, deve existir uma clara definição das responsabilidades e direcionamento dos requisitos pela área de negócios (o cliente) e um claro entendimento acerca do que e como precisa ser entregue pela TI (o fornecedor). A **Figura 6** ilustra como a estratégia da empresa deveria ser traduzida pela área de negócios em objetivos relacionados às iniciativas de TI (objetivos de negócios para TI). Esses objetivos devem levar a uma clara definição dos objetivos próprios da área de TI (os objetivos de TI), o que por sua vez irá definir os recursos e capacidades de TI (a arquitetura de TI para a organização) necessários para executar de maneira bem-sucedida a parte que cabe à TI na estratégia da empresa. [1]

Figura 6 - Definindo os objetivos de TI e a Arquitetura da Empresa para TI



Uma vez que os objetivos alinhados estiverem definidos, eles precisam ser monitorados para assegurar que as entregas atendam às expectativas. Isto é alcançado por métricas derivadas dos objetivos e capturadas pelo *scorecard* de TI.

Para que o cliente entenda os objetivos de TI e o *scorecard* de TI, todos esses objetivos e métricas associadas devem ser expressos em termos de negócios significativos para o cliente. Combinado com um efetivo alinhamento da hierarquia dos objetivos, isto irá assegurar que os negócios confirmem que TI irá provavelmente colaborar para que a empresa atinja seus objetivos.

O Apêndice I 015 – Tabelas Relacionando os Objetivos e Processos – apresenta uma visão global de como os objetivos genéricos de negócios relacionam-se com os objetivos, processos e critérios de informação de TI. As tabelas ajudam a demonstrar o escopo do COBIT e o relacionamento geral dos negócios entre o COBIT e o direcionamento a empresa. Como ilustrado na **figura 6**, esses direcionamentos derivam dos negócios e dos níveis de governança da empresa, o primeiro focando mais na funcionalidade e velocidade da entrega, enquanto que o último foca mais em eficiência dos custos, retorno do investimento (ROI) e aderência.

[1] É necessário mencionar que a definição e a implementação de uma arquitetura corporativa de TI também criarão objetivos internos de TI que contribuem para os objetivos de negócios, mas não são diretamente derivados desses objetivos.

RECURSOS DE TI

A organização de TI entrega de acordo com esses objetivos por um conjunto claramente definido de processos que usam a experiência das pessoas e a infra-estrutura tecnológica para processar aplicativos de negócios de maneira automatizada, aprimorando as informações de negócios. Esses recursos em conjunto com os processos constituem a arquitetura de TI da organização, como demonstrado na figura 6.

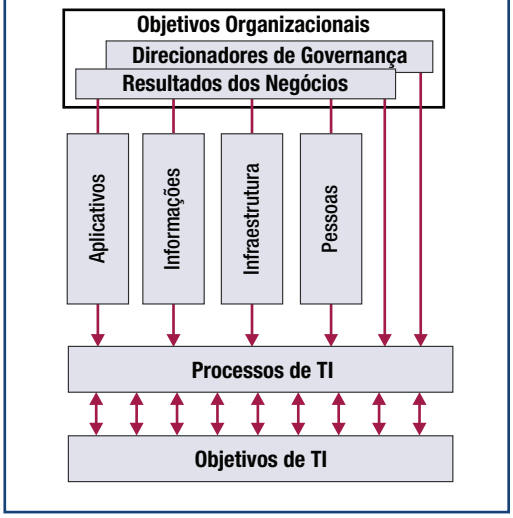
Para atender aos requisitos de negócios para TI, a organização precisa investir nos recursos necessários para criar uma adequada capacidade técnica (ex. um sistema de planejamento de recursos [ERP]) que atenda a uma necessidade de negócios (ex. implementar um canal de suprimentos) resultando no desejado retorno (ex. aumento de vendas e benefícios financeiros).

Os recursos de TI identificados no CobiT podem ser definidos como segue:

- **Aplicativos** são os sistemas automatizados para usuários e os procedimentos manuais que processam as informações.
- **Informações** são os dados em todas as suas formas, a entrada, o processamento e a saída fornecida pelo sistema de informação em qualquer formato a ser utilizado pelos negócios.
- **Infraestrutura** refere-se à tecnologia e aos recursos (ou seja, hardware, sistemas operacionais, sistemas de gerenciamento de bases de dados, redes, multimídia e os ambientes que abrigam e dão suporte a eles) que possibilitam o processamento dos aplicativos.
- **Pessoas** são os funcionários requeridos para planejar, organizar, adquirir, implementar, entregar, suportar, monitorar e avaliar os sistemas de informação e serviços. Eles podem ser internos, terceirizados ou contratados, conforme necessário.

A **Figura 7** mostra como os objetivos de negócios para TI influenciam o modo como os recursos de TI precisam ser gerenciados pelos processos de TI para entregar os objetivos de TI.

Figura 7 - Gerenciando os Recursos de TI para Entregar os Objetivos de TI



Orientado para processos

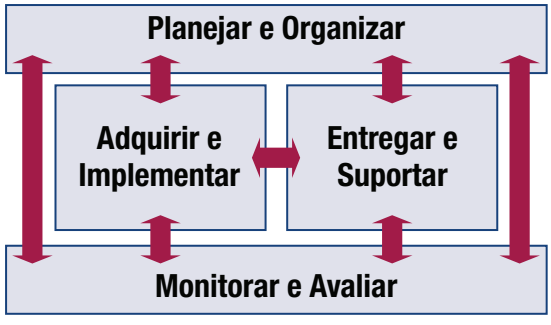
O CobiT define as atividades de TI em um modelo de processos genéricos com quatro domínios. Esses domínios são Planejar e Organizar, Adquirir e Implementar, Entregar e Suportar e Monitorar e Avaliar. Esses domínios mapeiam as tradicionais áreas de responsabilidade de TI de planejamento, construção, processamento e monitoramento.

O modelo CobiT fornece um modelo de processo de referência e uma linguagem comum para que todos na organização possam visualizar e gerenciar as atividades de TI. Incorporar o modelo operacional e a linguagem comum para todas as áreas de negócios envolvidas em TI é um dos mais importantes passos e ações preliminares para uma boa governança. Isto também fornece uma metodologia para medição e monitoramento da performance de TI, comunicação com provedores de serviços e integração das melhores práticas de gerenciamento. Um modelo de processos incentiva a determinação de proprietários dos processos, o que possibilita a definição de responsabilidades.

Para que a governança de TI seja eficiente, é importante avaliar as atividades e riscos da TI que precisam ser gerenciados. Geralmente eles são ordenados por domínios de responsabilidade de planejamento, construção, processamento e monitoramento. No modelo CobiT esses domínios, como demonstrado na Figura 8, são denominados:

- **Planejar e Organizar (PO)** - Provê direção para entrega de soluções (AI) e entrega de serviços (DS)
- **Adquirir e Implementar (AI)** - Provê as soluções e as transfere para tornarem-se serviços
- **Entregar e Suportar (DS)** - Recebe as soluções e as torna passíveis de uso pelos usuários finais
- **Monitorar e Avaliar (ME)** - Monitora todos os processos para garantir que a direção definida seja seguida.

Figura 8 - Os Quatro Domínios Inter-relacionados do CobiT



PLANEJAR E ORGANIZAR (PO)

Este domínio cobre a estratégia e as táticas, preocupando-se com a identificação da maneira em que TI pode melhor contribuir para atingir os objetivos de negócios. O sucesso da visão estratégica precisa ser planejado, comunicado e gerenciado por diferentes perspectivas. Uma apropriada organização bem como uma adequada infraestrutura tecnológica devem ser colocadas em funcionamento. Este domínio tipicamente ajuda a responder as seguintes questões gerenciais:

- As estratégias de TI e de negócios estão alinhadas?
- A empresa está obtendo um ótimo uso dos seus recursos?
- Todos na organização entendem os objetivos de TI?
- Os riscos de TI são entendidos e estão sendo gerenciados?
- A qualidade dos sistemas de TI é adequada às necessidades de negócios?

ADQUIRIR E IMPLEMENTAR (AI)
Para executar a estratégia de TI, as soluções de TI precisam ser identificadas, desenvolvidas ou adquiridas, implementas e integradas ao processo de negócios. Além disso, alterações e manutenções nos sistemas existentes são cobertas por esse domínio para assegurar que as soluções continuem a atender aos objetivos de negócios. Este domínio tipicamente trata das seguintes questões de gerenciamento:
- Os novos projetos fornecerão soluções que atendam às necessidades de negócios?
- Os novos projetos serão entregues no tempo e orçamento previstos?
- Os novos sistemas ocorreram apropriadamente quando implementado?
- As alterações ocorrerão sem afetar as operações de negócios atuais?

ENTREGAR E SUPORTAR (DS)
Este domínio trata da entrega dos serviços solicitados, o que inclui entrega de serviço, gerenciamento da segurança e continuidade, serviços de suporte para os usuários e o gerenciamento de dados e recursos operacionais. Trata geralmente das seguintes questões de gerenciamento:
- Os serviços de TI estão sendo entregues de acordo com as prioridades de negócios?
- Os custos de TI estão otimizados?
- A força de trabalho está habilitada para utilizar os sistemas de TI de maneira produtiva e segura?
- Os aspectos de confidencialidade, integridade e disponibilidade estão sendo contemplados para garantir a segurança da informação?

MONITORAR E AVALIAR (ME)
Todos os processos de TI precisam ser regularmente avaliados com o passar do tempo para assegurar a qualidade e a aderência aos requisitos de controle. Este domínio aborda o gerenciamento de performance, o monitoramento do controle interno, a aderência regulatória e a governança. Trata geralmente das seguintes questões de gerenciamento:
- A performance de TI é mensurada para detectar problemas antes que seja muito tarde?
- O gerenciamento assegura que os controles internos sejam efetivos e eficientes?
- O desempenho da TI pode ser associado aos objetivos de negócio?
- Existem controles adequados para garantir confidencialidade, integridade e disponibilidade das informações?

Dentro desses quatro domínios o COBIT identificou 34 processos de TI geralmente utilizados (veja a **Figura 23** para uma lista completa). Embora a maioria das organizações tenha definido as responsabilidades de TI de planejar, construir, processar e monitorar, e muitas delas tenham os mesmos processos-chave, poucas terão a mesma estrutura de processos ou aplicarão todos os 34 processos do COBIT. O COBIT fornece uma completa lista de processos que podem ser utilizados para verificar a totalidade das atividade e responsabilidades. No entanto, nem todos precisam ser aplicados e podem ser combinados conforme as necessidades de cada empresa.

Para cada um desses 34 processos, uma ligação foi feita com os objetivos de negócios e de TI suportados. Também são fornecidas informações sobre como os objetivos podem ser medidos, quais são as atividades-chave, as principais entregas e quem é responsável por elas.

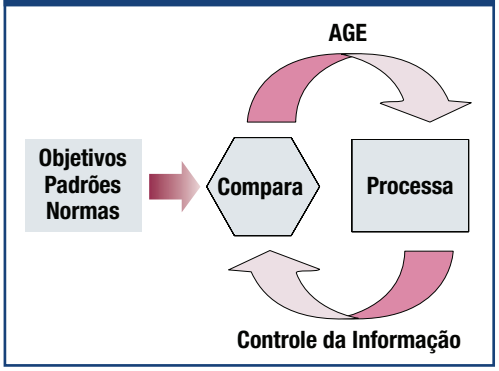
Baseado em Controles
O COBIT define objetivos de controles para todos os 34 processos e engloba todos os processos e controles de aplicativos.

PROCESSOS PRECISAM DE CONTROLES
Controle é definido como políticas, procedimentos, práticas e estruturas organizacionais criadas para prover uma razoável garantia de que os objetivos de negócios serão atingidos e que eventos indesejáveis serão evitados ou detectados e corrigidos.

Os objetivos de controle de TI fornecem um conjunto completo de requisitos de alto nível a serem considerados pelos executivos para um controle efetivo de cada processo de TI. Eles:
- São definições de ações gerenciais para aumentar o valor ou reduzir o risco
- Consistem em políticas, procedimentos, práticas e estruturas organizacionais
- São desenvolvidos para prover uma razoável garantia de que os objetivos de controle serão atingidos e que eventos indesejáveis serão evitados ou detectados e corrigidos

A empresa precisa fazer escolhas relacionadas a esses processos ao:
- Selecionar aqueles que são aplicáveis
- Decidir quais deles serão implementados
- Escolher como implementá-los (frequência, abrangência, automação, etc.)
- Aceitar o risco de não implementar aqueles que podem ser aplicáveis

Figura 9 - Modelo de Controle



Uma diretriz pode ser obtida no modelo padrão de controle apresentado na **Figura 9**. Ele segue o principio evidente na seguinte analogia: Quando a temperatura da sala (padrão) do sistema de aquecimento (processo) está definida, o sistema irá constantemente averiguar (comparar) a temperatura ambiente da sala (controle de informação) e irá sinalizar (agir) para o sistema de aquecimento para prover mais ou menos calor.

Os gerentes operacionais usam os processos para organizar e gerenciar as atividades de TI em andamento. O CobiT provê um modelo de processo genérico que representa todos os processos normalmente encontrados nas funções de TI, fornecendo um modelo referência comum compreensível para os gerentes das operações de TI e de negócios. Para atingir uma governança efetiva, os controles precisam ser implementados pelos gerentes operacionais de acordo com um método definido de controles para todos os processos de TI. Uma vez que os controles de TI do CobiT são organizados por processos de TI, o método fornece uma ligação clara em relação aos requisitos de governança, processos e controles de TI.

Cada um dos processos de TI do CobiT possui uma descrição do processo e um número do objetivo de controle. No todo, eles formam as características de um processo bem gerenciado.

Os objetivos de controles são identificados por duas letras para identificar o domínio (PO, AI, DS e ME), um número de processo e um número de objetivo de controle. Além dos objetivos de controle, cada processo do CobiT possui requisitos de controle genéricos identificados por PC(n), que indica o número de controle do processo. Eles devem ser considerados junto com os objetivos de controle dos processos para que se tenha uma visão completa dos requisitos de controle.

PC1 Metas e Objetivos do Processo
Define e comunica as metas e objetivos específicos, mensuráveis, acionáveis, realísticos, orientados a resultados e no tempo apropriado (SMARRT) para a efetiva execução de cada processo de TI. Assegura que eles estão ligados aos objetivos de negócios e que são suportados por métricas apropriadas.

PC2 Propriedade dos Processos
Designa um proprietário para cada processo de TI e claramente define os papéis e responsabilidades de cada proprietário de processo. Inclui por exemplo, a responsabilidade pela elaboração do processo, interação com outros processos, responsabilidade pelos resultados finais, medidas da performance do processo e a identificação de oportunidades de melhorias.

PC3 Repetibilidade dos Processos
Elabora e estabelece cada processo-chave de TI de maneira que possa ser repetido e produzir de maneira consistente os resultados esperados. Fornece uma sequência lógica mas flexível das atividades que levarão ao resultado desejado, sendo ágil o suficiente para lidar com exceções e emergências. Usa processos consistentes, quando possível, e processos personalizados apenas quando inevitável.

PC4 Papéis e Responsabilidades
Define as atividades-chaves e as entregas do processo. Designa e comunica papéis e responsabilidades para uma efetiva e eficiente execução das atividades-chaves e sua documentação bem como a responsabilização pelo processo e suas entregas.

PC5 Políticas Planos e Procedimentos
Define e comunica como todas as políticas, planos e procedimentos que direcionam os processos de TI são documentados, revisados, mantidos, aprovados, armazenados, comunicados e utilizados para treinamento. Designa responsabilidades para cada uma dessas atividades e em momentos apropriados verifica se elas são executadas corretamente. Assegura que as políticas, planos e procedimentos sejam acessíveis, corretos, entendidos e atualizados.

PC6 Melhoria do Processo de Performance
Identifica um conjunto de métricas que fornecem direcionamento para os resultados e performance dos processos. Estabelece metas que refletem nos objetivos dos processos e indicadores de performance que permitem atingir os objetivos dos processos. Definem como os dados são obtidos. Compara as medições reais com as metas e toma medidas quanto aos desvios quando necessário. Alinha métricas, metas e métodos com o enfoque de monitoramento de performance geral de TI.

Controles efetivos reduzem riscos, aumentam a probabilidade da entrega de valor e aprimoram a eficiência, pois existirão poucos erros e o enfoque de gerenciamento será mais consistente.

Além disso, o CobiT traz exemplos de cada processo que são ilustrativos, mas não definidores ou completos, de:
Entradas e saídas em geral
- Atividades e orientações sobre papéis e responsabilidades em uma tabela que indica quem é responsável, responsabilizado, consultado e informado (RACI).
- Principais objetivos da atividade (o que de mais importante deve ser feito).
- Métricas

Além de avaliar quais controles são necessários, os proprietários dos processos devem entender quais entradas eles precisam receber de outros e o que os outros precisam de seu processo. O CobiT fornece exemplos de entradas e saídas básicos que servem para qualquer processo, incluindo requisitos externos de TI. Existem alguns tipos de saída que servem de entrada para todos os outros processos, os quais são marcados como "ALL" nas tabelas de saídas e, portanto, não são mencionados como entradas para todos os processos. Geralmente incluem os padrões de qualidade e requisitos de métricas, a estrutura do processo de TI, os papéis e responsabilidades documentados, a estrutura de controle de TI da organização, as políticas de TI e as funções e responsabilidades dos funcionários.

O entendimento dos papéis e responsabilidades de cada processo é essencial para uma efetiva governança. O CobiT provê a tabela RACI para cada processo. O termo Responsabilizado significa que "a responsabilidade é deste indivíduo" – esta é a pessoa que dá orientações e autoriza uma atividade. A responsabilidade é atribuída à pessoa que faz com que a tarefa seja executada. Os outros dois papéis (consultado e informado) asseguram que todos que precisam serão envolvidos e suportam o processo.

CONTROLES DE NEGÓCIOS E DE TI

Os sistemas de controles internos das organizações afetam a área de TI em três níveis:

- No nível da Alta Direção, os objetivos de negócios e as políticas são definidos e decisões são tomadas em relação a como entregar e gerenciar os recursos da organização para executar a estratégia. O enfoque geral para a governança e o controle é definido pela Alta Direção e comunicado para toda a organização. O ambiente de controle de TI é direcionado por estes objetivos e políticas de alto nível.
- No nível dos processos de negócios, os controles são aplicados às atividades específicas dos negócios. A maioria dos processos de negócios é automatizada e integrada aos sistemas aplicativos de TI. No entanto, alguns controles existentes no processo de negócios permanecem como procedimentos manuais, tais como a autorização para transações, a segregação de funções e as reconciliações manuais. Portanto, os controles no nível dos processos de negócios são uma combinação de controles manuais conduzidos pela área de negócios e controles de negócios e de aplicativos automatizados. Ambos são de responsabilidade da área de negócios no que se refere a definição e gerenciamento, embora os controles dos aplicativos exijam a participação da área de TI no seu projeto e desenvolvimento.
- Para suportar os processos de negócios, a área de TI fornece serviços de TI, usualmente de maneira compartilhada para diversos processos de negócios, uma vez que muitos processos de desenvolvimento e operacionais de TI são supridos para toda a organização e boa parte da infra-estrutura de TI é provida como um serviço comum (por exemplo, redes, bases de dados, sistemas operacionais e armazenamento). Os controles aplicados a todas as atividades de serviços de TI chamados de controles gerais de TI. A operação confiável desses controles é necessária para que se possa confiar nos controles existentes nos aplicativos. Por exemplo, um gerenciamento de mudanças insatisfatório poderia prejudicar (acidental ou deliberadamente) a confiança depositada em testes de integridade automáticos.

CONTROLES GERAIS DE TI E CONTROLES DE APLICATIVOS

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

- Desenvolvimento de sistemas
- Gerenciamento de mudanças
- Segurança
- Operação de computadores

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

- Totalidade
- Veracidade
- Validade
- Autorização
- Segregação de funções

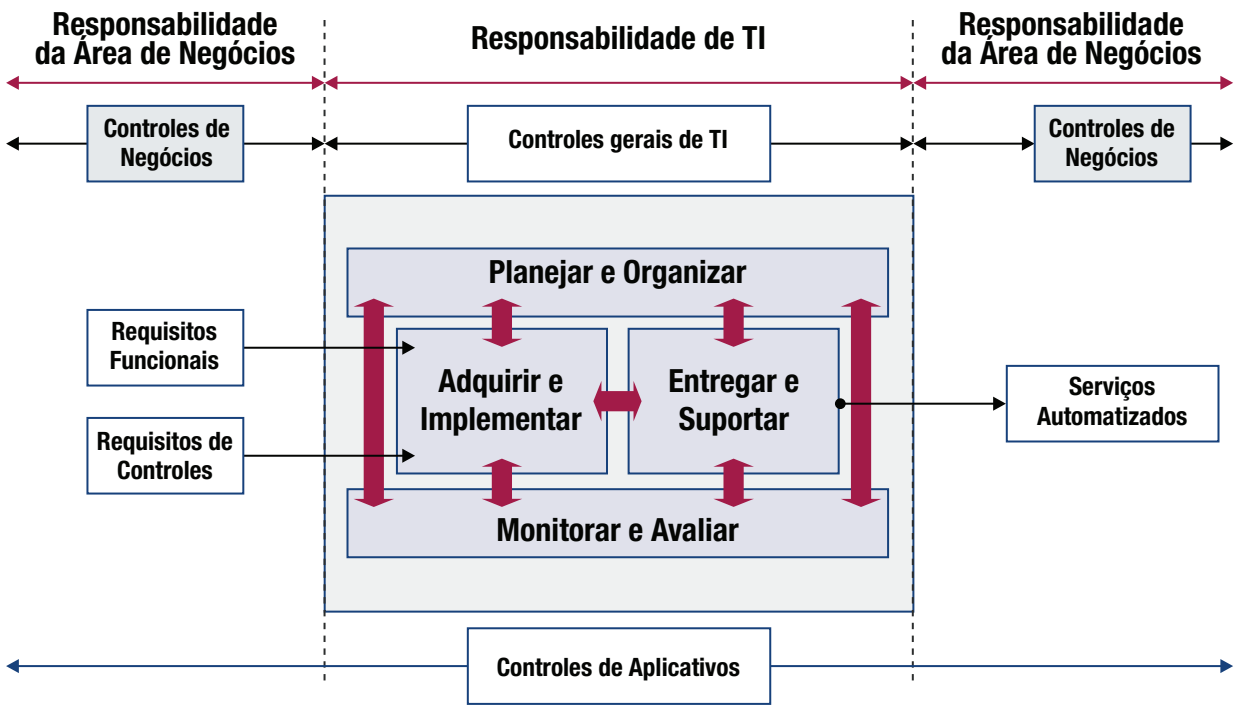
O CobiT assume que o projeto e a implementação dos controles automatizados em aplicativos é de responsabilidade da área de TI, cobertos no domínio Aquisição e Implementação, com base nos requisitos de negócios definidos a partir dos critérios de informação do CobiT, como demonstrado na Figura 10. A responsabilidade pelo controle e o gerenciamento operacional dos controles de aplicativos não é da área de TI, mas do proprietário do processo de negócio.

Assim, a responsabilidade pelos controles de aplicativos é compartilhada entre as áreas de negócios e de TI, mas a natureza das responsabilidades muda, como segue:

- A área de negócios é responsável por:
  - Definir os requisitos funcionais e de controles
  - Utilizar os serviços automatizados
- A área de TI é responsável por:
  - Automatizar e implementar os requisitos funcionais e de controles
  - Estabelecer controles para manter a integridade dos controles de aplicativos

Portanto os processos de TI do CobiT cobrem os controles gerais de TI, mas somente os aspectos do desenvolvimento dos controles de aplicativos; a responsabilidade pela definição e o uso operacional é da área de negócio.

Figura 10 - Fronteiras de Negócios, Controles Gerais e de Aplicativos



A lista a seguir apresenta um conjunto recomendado de objetivos de controles de aplicativos. Eles são identificados como “ACn” , que significa o número do controle de aplicação.

AC1 Preparação e Autorização de Dados Originais
Assegura que os documentos fonte sejam preparados por pessoal autorizado e qualificado seguindo os procedimentos estabelecidos, levando em consideração uma adequada segregação de funções relacionadas com a criação e aprovação desses documentos. Erros e omissões podem ser minimizados através de bom desenho de formulário para entrada da informação, permitindo que erros e irregularidades detectados sejam reportados e corrigidos.

AC2 Entrada e Coleta de Dados Fontes
Estabelece que a entrada de dados seja executada de maneira apropriada por pessoal autorizado e qualificado. A correção e o reenvio de dados que foram erroneamente inseridos devem ser executados sem comprometer o nível de autorização da transação original. Quando apropriado para a reconstrução, os documentos originais devem ser guardados por um período adequado.

AC3 Testes de Veracidade, Totalidade e Autenticidade
Assegura que as transações sejam exatas, completas e válidas. Valida os dados que foram inseridos e editados ou enviados de volta para correção o mais próximo possível do ponto onde foram originados.

AC4 Processamento Íntegro e Válido
Mantém a integridade e validade dos dados no ciclo de processamento. A detecção de transações errôneas não interrompe o processamento de transações válidas.

AC5 Revisão das Saídas, Reconciliação e Manuseio de Erros
Estabelece procedimentos e responsabilidades associadas para assegurar que as saídas sejam manuseadas de uma forma autorizada, entregues para os destinatários corretos e protegidas durante a transmissão. Garante que ocorre a verificação, detecção e correção da exatidão das saídas e que a informação provida pela saída é usada.

AC6 Autenticação e Integridade das Transações
Antes de transportar os dados das transações entre os aplicativos e as funções de negócios/operacionais (internas ou externas à organização), verifica endereçamento adequado, autenticidade da origem e integridade do conteúdo. Mantém a autenticidade e integridade durante a transmissão ou transporte.

Direcionamento Baseado em Medição

Uma necessidade básica para toda organização é entender a situação dos seus próprios sistemas de TI e decidir que nível de gerenciamento e controle a empresa deveria ter. Para decidir dentro de um nível correto, os executivos devem se perguntar: Quão distante devemos ir e será que o custo é justificado pelo benefício?

Obter uma visão objetiva do nível de performance da própria organização não é fácil. O que deve ser avaliado e como? As organizações precisam avaliar onde elas e onde são requeridas melhorias, bem como implementar um conjunto de ferramentas de gerenciamento para atingir esse aprimoramentos. O CobiT lida com essas questões por fornecer:

- Modelos de maturidade que permitem fazer comparações e identificar os necessários aprimoramentos de capacidades,
- Objetivos de performance e métricas para os processos de TI, demonstrando como os processos atingem os objetivos de negócios e de TI e são utilizados para mensurar a performance dos processos internos baseados nos princípios do *balanced scorecard*
- Objetivo de atividades para habilitar o efetivo desempenho do processo

MODELOS DE MATURIDADE

A Alta Direção de corporações e de grandes organizações é cada vez mais solicitada a considerar quão bem a área de TI está sendo gerenciada. Em resposta, planos de negócios requerem o desenvolvimento de melhorias e um apropriado gerenciamento e controle sobre a infra-estrutura de informação. Enquanto alguns argumentariam que isso não é algo importante, é preciso considerar o custo-benefício e as seguintes questões relacionadas:

- O que os nossos concorrentes estão fazendo e como estamos posicionados em relação a eles?
- Quais são as boas práticas aceitáveis para o ambiente de negócio e como estamos colocados em relação a essas práticas?
- Com base nessas comparações, podemos dizer que estamos fazendo o suficiente?
- Como podemos identificar o que precisa ser feito para atingir um nível adequado de gerenciamento e controle sobre os processos de TI?

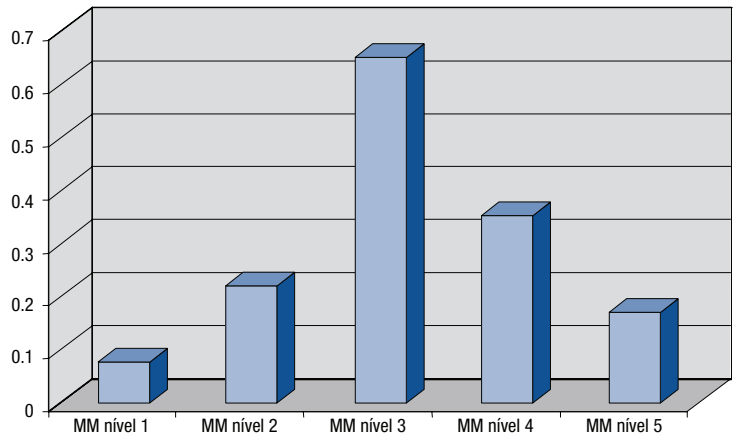
Pode ser difícil fornecer respostas significativas para essas questões. O gerenciamento de TI está constantemente procurando ferramentas de benchmarking e de autoavaliação em resposta à necessidade de saber o que fazer de maneira eficiente. Começando com os processos CobiT, o proprietário do processo poderá gradativamente ampliar as comparações com os objetivos de controle. Isso atende a três necessidades:

1. Uma medida relativa de onde a empresa está
2. Uma maneira de eficientemente decidir para onde ir
3. Uma ferramenta para avaliação do progresso em relação às metas

O modelo de maturidade para o gerenciamento e controle dos processos de TI é baseado num método de avaliar a organização, permitindo que ela seja pontuada de um nível de maturidade não-existente (0) a otimizado (5). Este enfoque é derivado do modelo de maturidade do Software Engineering Institute (SEI) definido para a maturidade da capacidade de desenvolvimento de software. Embora siga os conceitos do SEI, a implementação CobiT difere consideravelmente do original do SEI, o qual era orientado para os princípios de engenharia de produtos de software, organizações buscando excelência nessas áreas e uma avaliação formal dos níveis de maturidade para que os desenvolvedores de software pudessem ser "certificados". No CobiT, uma definição genérica é provida para as escalas de maturidade do CobiT as quais são similares às do CMM mas interpretadas de acordo com a natureza dos processos de gerenciamento de TI do CobiT. Um modelo específico é fornecido derivando dessa escala genérica para cada um dos 34 processos CobiT. Independente do modelo, as escalas não devem ser tão granulares visto que seria difícil de utilizar e sugeriria um precisão não justificável, por que em geral o propósito é identificar onde estão as questões e como definir prioridades para aprimoramentos. O propósito não é avaliar o nível de aderência aos objetivos de controles.

Os níveis de maturidade são designados como perfis de processos de TI que a empresa reconheceria como descrição de possíveis situações atuais e futuras. Eles não são designados como um modelo inicial, onde não se pode avançar para o próximo nível sem antes ter cumprido todas as condições do nível inferior. Com os modelos de maturidade do CobiT, diferentemente do enfoque original SEI CMM, não há intenção de medir os níveis de maneira precisa ou tentar certificar que aquele nível foi exatamente atingido. A avaliação de maturidade do CobiT espera resultar em um perfil em que as condições relevantes para diversos níveis de maturidade serão atingidas, como demonstrado no gráfico de exemplo da **Figura 11**.

Figura 11 - Possível Nível de Maturidade de um Processo de TI



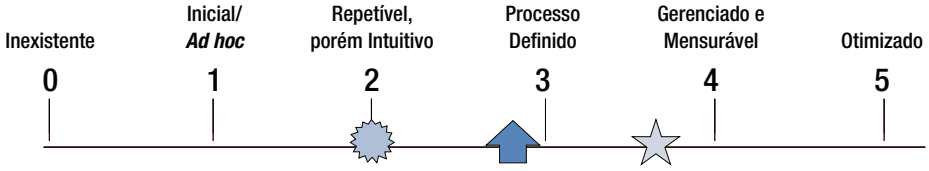
Possível Nível de Maturidade de um Processo de TI: O exemplo ilustra um processo que está amplamente situado no nível 3 mas que ainda tem algumas questões de aderência como os requerimentos de nível mais baixo, embora já esteja investindo na medição de performance (nível 4) e em otimização (nível5)

Isto ocorre porque quando aplicamos a avaliação de maturidade usando o CobiT, às vezes uma implementação estará em andamento em diferentes níveis mesmo que não de maneira completa e suficiente. Esses pontos fortes podem ser trabalhados para aprimorar a maturidade. Por exemplo, algumas partes do processo podem estar bem definidas e mesmo estando incompletas, seria enganoso afirmar que o processo não está definido.

Ao utilizar os modelos de maturidade desenvolvidos para cada um dos 34 processos de TI do CobiT, a gerencia pode identificar:
- O estágio atual de performance da empresa – Onde a empresa está hoje
- O estágio atual do mercado – A comparação
- A meta de aprimoramento da empresa – Onde a empresa quer estar
- O caminho de crescimento entre o "como está" e "como será"

Para tornar os resultados mais facilmente utilizáveis em sumários gerenciais, onde serão mostrados como meio de suporte para planos de negócios *(business cases)*, um método de apresentação é necessário (**Figura 12**).

Figura 12 - Representação Gráfica dos Modelos de Maturidade



LEGENDAS PARA OS SÍMBOLOS UTILIZADOS

Estágio atual da empresa

Média do mercado

Meta da empresa

LEGENDA UTILIZADA PARA MEDIÇÃO

0 - Gerenciamento de processos não aplicado.
1 - Processos são *ad hoc* e desorganizados.
2 - Processos seguem um caminho padrão.
3 - Processos são documentados e comunicados.
4 - Processos são monitorados e medidos.
5 - Boas práticas são seguidas e automatizadas.

O desenvolvimento dessa representação gráfica foi baseado nas descrições genéricas do modelo de maturidade demonstradas na **Figura 13**.

O modelo CobiT para o gerenciamento de processos de TI foi desenvolvido como uma ênfase forte em controles. Essas escalas precisam ser práticas para serem aplicadas e de fácil entendimento. O assunto gerenciamento de processos de TI é inerentemente complexo e subjetivo e portanto, é mais bem tratado através de avaliações facilitadas que provocam a consciência, capturam o consenso geral e motivam o aprimoramento. Essas avaliações podem ser executadas com base nas descrições do nível de maturidade como um todo ou com um maior rigor contra cada uma das afirmações individuais dessas descrições. Seja qual for o caminho escolhido, é preciso ter experiência no processo que está sendo revisado.

A vantagem de uma abordagem de modelo de maturidade é a relativa facilidade de os gerentes colocarem-se a si mesmos em uma escala e avaliar o que está envolvido no aprimoramento da performance, se necessário. As escalas incluem o 0, pois é possível que um processo não exista de fato. A escada de 0 a 5 é baseada em uma escala simples de maturidade, demonstrando como um processo evolui de capacidade inexistente para capacidade otimizada.

No entanto o processo de gerenciamento de capacidade não é o mesmo que a performance do processo. As capacidades requeridas como determinado pelos objetivos de negócios e de TI podem não ser aplicadas no mesmo nível em todo o ambiente de TI, ou seja, não de forma consistente ou somente para um limitado número de sistemas ou unidades. A medição de performance como visto nos próximos parágrafos é essencial para determinar a performance atual da empresa nos seus processos de TI.

Figura 13 - Modelo de Maturidade Genérico

0 Inexistente – Completa falta de um processo reconhecido. A empresa nem mesmo reconheceu que existe uma questão a ser trabalhada.

1 Inicial / *Ad hoc* – Existem evidências que a empresa reconheceu que existem questões e que precisam ser trabalhadas. No entanto, não existe processo padronizado; ao contrário, existem enfoques *Ad Hoc* que tendem a ser aplicados individualmente ou caso-a-caso. O enfoque geral de gerenciamento é desorganizado.

2 Repetível, porém Intuitivo – Os processos evoluíram para um estágio onde procedimentos similares são seguidos por diferentes pessoas fazendo a mesma tarefa. Não existe um treinamento formal ou uma comunicação dos procedimentos padronizados e a responsabilidade é deixado com o indivíduo. Há um alto grau de confiança no conhecimento dos indivíduos e conseqüentemente erros podem ocorrer.

3 Processo Definido – Procedimentos foram padronizados, documentados e comunicados através de treinamento. É mandatório que esses processos sejam seguidos; no entanto, possivelmente desvios não serão detectados. Os procedimentos não são sofisticados mas existe a formalização das práticas existentes.

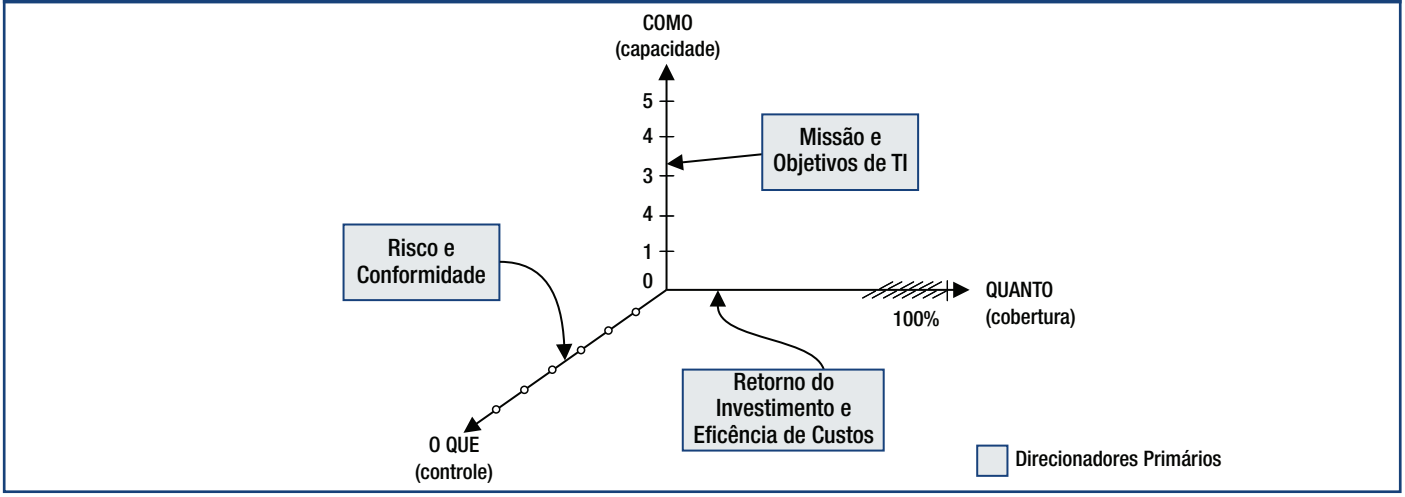
4 Gerenciado e Mensurável – A gerencia monitora e mede a aderência aos procedimentos e adota ações onde os processos parecem não estar funcionando muito bem. Os processos estão debaixo de um constante aprimoramento e fornecem boas práticas. Automação e ferramentas são utilizadas de uma maneira limitada ou fragmentada.

5 Otimizado – Os processos foram refinados a um nível de boas práticas, baseado no resultado de um contínuo aprimoramento e modelagem da maturidade como outras organizações. TI é utilizada como um caminho integrado para automatizar o fluxo de trabalho, provendo ferramentas para aprimorar a qualidade e efetividade, tornando a organização rápida em adaptar-se.

Embora uma capacidade apropriadamente aplicada já reduza riscos, a organização ainda precisa analisar quais os controles necessários para assegurar que os riscos sejam mitigados e que valor é obtido em linha com o apetite de risco e objetivos de negócios. Esses controles são guiados pelos objetivos de controle do COBIT. O Apêndice III provê um modelo de maturidade de controles internos que ilustram a maturidade de uma empresa em relação ao estabelecimento e performance dos controles internos. Às vezes a análise é iniciada em resposta a vários direcionamentos externos, mas preferencialmente deve ser inserida e documentada pelos processos PO6 Comunicar as Diretrizes e Expectativas da Diretoria e ME2 Monitorar e Avaliar os Controles Internos do COBIT.

Capacidade, cobertura e controle são todas a dimensões do processo de maturidade, como ilustrado na **figura 14.**

Figura 14 - As três Dimensões da Maturidade



O modelo de maturidade é uma forma de medir quão bom os processos de gerenciamento são, ou seja, quão capazes eles são. O quanto devem ser desenvolvidos ou capacitados deveria primariamente depender dos objetivos de TI e sua conexão como as necessidades de negócios que eles suportam. O quanto dessa capacidade é realmente entregue depende largamente do retorno que a organização deseja do investimento. Por exemplo, existem processos e sistemas críticos que precisam de um gerenciamento da segurança maior e mais restrito do que outros que são menos críticos. Por outro lado, o grau de sofisticação dos controles que precisam ser aplicados em um processo é mais direcionado pelo apetite de risco da organização e pelos requisitos aplicáveis de conformidade.

A escala do modelo de maturidade ajudará os profissionais a explicar aos gerentes onde existem deficiências no gerenciamento do processo de TI e definir metas de onde querem estar. O correto nível de maturidade será influenciado pelos objetivos de negócios, o ambiente operacional e as práticas do mercado. Especificamente, o nível de maturidade gerencial dependerá da dependência da empresa em TI, de sua sofisticação tecnológica e, mais importante, do valor da informação.

Um ponto de referência estratégico para uma empresa aprimorar o gerenciamento e o controle dos processos de TI pode ser encontrado ao se atentar para os recentes padrões internacionais e boas práticas reconhecidas. As práticas mais atuais podem se tornar o nível esperado de performance para o futuro e portanto são úteis para planejar onde a empresa espera estar com o passar do tempo.

Os modelos de maturidade são construídos a partir do modelo qualitativo genérico (veja **Figura 13**) no qual os princípios dos seguintes atributos são adicionados de maneira crescente através dos níveis:
- Consciência e comunicação
- Políticas, planos e procedimentos
- Ferramentas e automação
- Habilidades e especialização
- Responsabilidade e responsabilização
- Definição de objetivos e medição

A tabela de atributos de maturidade na **Figura 15** relaciona as características de como os processos de TI são gerenciados e descreve como eles evoluem de um processo inexistente para um otimizado. Esses atributos podem ser usados para uma avaliação mais abrangente, análise de deficiências e plano de aprimoramento.

Em resumo, os modelos de maturidade fornecem um perfil genérico de estágios através dos quais cada empresa pode evoluir em gerenciamento e controle de processos de TI. Eles são:
- Um conjunto de requisitos e aspectos que habilitam os diferentes níveis de maturidade
- Uma escala onde a diferença pode ser facilmente medida
- Uma escala que pode ser utilizada para comparações pragmáticas
- Uma base para definir as posições “como está” e de “como será”
- Suporte para a análise de deficiências a fim de determinar o que precisa ser feito para atingir o nível escolhido
- Considerada no conjunto, uma visão de como a área de TI é gerenciada na organização

Os modelos de maturidade do CobiT enfocam a maturidade mas não necessariamente a abrangência e profundidade dos controles. Eles não são um número para ser atingido, tampouco são desenhados para ser uma base formal de certificação com níveis que criam requisitos mínimos difíceis de atingir. No entanto, são desenhados para serem sempre aplicáveis, fornecendo níveis com descrições que uma empresa pode reconhecer como os que melhor se adequam aos seus processos. O nível correto é determinado pelo tipo de organização, ambiente e estratégia.

A abrangência e a profundidade do controle e como a capacidade é utilizada e entregue são decisões de custo-benefício. Por exemplo, um alto nível de gerenciamento de segurança pode ter que ser enfatizado apenas nos sistemas mais críticos da organização. Outro exemplo seria a escolha entre uma revisão semanal e um controle contínuo automatizado.

Finalmente, embora altos níveis de maturidade aumentem o controle sobre os processos, a organização ainda precisa analisar, com base nos riscos e direcionamento de valor, quais mecanismos devem ser aplicáveis. Os objetivos genéricos de negócios e de TI definidos nessa metodologia ajudarão na análise. Os mecanismos de controle são guiados pelos objetivos de controle do CobiT e enfocam o que é feito no processo; os modelos de maturidade primariamente focam em quão bem os processos são gerenciados. O Apêndice III apresenta um modelo de maturidade genérico que demonstra o estágio do ambiente de controle e o estabelecimento de controles internos de uma empresa.

Um ambiente de controle apropriadamente implementado é obtido quando se observam todos os três aspectos da maturidade (capacidade, abrangência e controle). Melhorar a maturidade reduz riscos e aprimora a eficiência, levando a uma menor quantidade de erros, processos mais previsíveis e uso eficiente dos recursos sob o ponto de vista de custos.

MEDIÇÃO DE PERFORMANCE

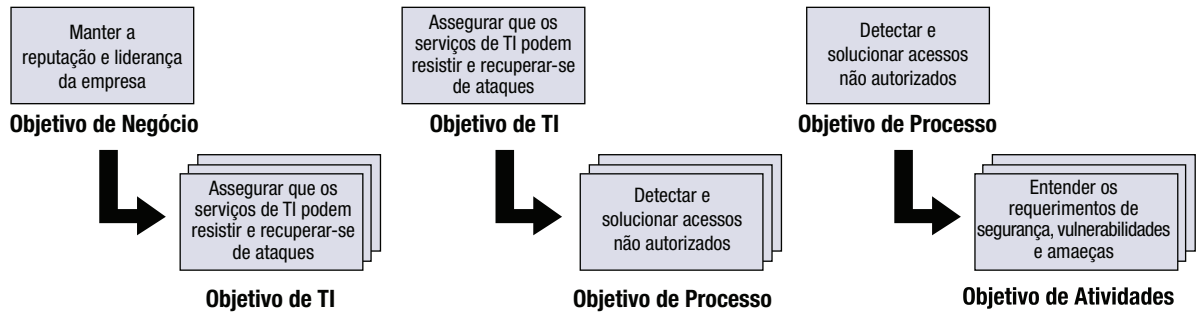
Os objetivos e métricas são definidos no CobiT em três níveis:
- Objetivos e métricas de TI que definem o que os negócios esperam de TI e como medir isso
- Objetivos e métricas dos processos que definem o que os processos de TI precisam entregar para suportar os objetivos de TI e como medir isso
- Objetivos e métricas de atividades que estabelecem o que precisa acontecer dentro do processo para atingir a requerida performance e como medir isso

Figura 15 - Tabela de Atributos de Maturidade

Consciência e Comunicação	Políticas, Planos e Procedimentos	Ferramentas e Automação	Habilidades e Especialização	Responsabilidade e Responsabilização	Definição de Objetivos e Métricas
1 Reconhecimento da necessidade do processo está surgindo. Existe uma comunicação esporádica das questões.	Existem enfoques *ad hoc* para processos e práticas. O processo e as políticas são indefinidas.	Algumas ferramentas podem existir; o uso é baseado em ferramentas padrões de microinformática. Não existe um enfoque planejado para uso de ferramentas.	Habilidades requeridas para o processo não são identificadas. Um plano de treinamento não existe e não ocorre treinamento formal.	Não existe definição de responsabilização e responsabilidade. Pessoas assumem propriedade de questões baseadas em suas próprias iniciativas de maneira reativa.	Os objetivos não são claros e não são utilizadas métricas.
2 Existe consciência da necessidade de agir. A gerencia comunica as questões genéricas.	Processos similares e comuns surgem, mas são amplamente intuitivos devido a habilidades individuais. Alguns aspectos do processo são repetíveis, podendo existir alguma documentação e entendimento informal da política e procedimentos.	Existe um enfoque comum para o uso de ferramentas mas está baseado em soluções desenvolvidas por pessoas chaves. Ferramentas de mercado podem ter sido adquiridas, mas provavelmente não utilizadas corretamente e podem ser de mercado.	Habilidades mínimas requeridas para áreas críticas são identificadas. Treinamento provido em resposta a necessidades, ao invés de baseado num plano concordado, ocorre treinamento informal baseado no dia-a-dia de trabalho.	Indivíduos assumem sua responsabilidade e são usualmente responsabilizados, mesmo que isto não esteja formalmente acordado. Existe confusão sobre responsabilidades quando ocorrem problemas e uma cultura de acusação tende a existir.	Alguma definição de objetivos ocorre; algumas métricas financeiras são estabelecidas mas são conhecidas somente pelos executivos. Existe um monitoramento inconsistente em áreas isoladas.
3 Existe um entendimento da necessidade de agir. O gerenciamento é mais formal e estruturado em sua comunicação.	O uso de boas práticas surge. O processo, políticas e procedimentos são definidos e documentados para todas as atividades chaves.	Foi definido um plano para o uso e padronização de ferramentas para automatizar o processo. Ferramentas são utilizadas para seus propósitos básicos, mas pode não ser totalmente de acordo com o plano concordado e podem não ser integradas entre si.	As habilidades requeridas são definidas e documentadas para todas as áreas. Um plano formal de treinamento foi desenvolvido, mas o treinamento formal ainda é baseado em iniciativas individuais.	A responsabilidade e responsabilização por processos estão definidas e proprietários de processos são identificados. O proprietário do processo possivelmente não tem total autoridade para exercer suas responsabilidades.	Alguns objetivos efetivos e métricas são definidos, mas não são comunicados e existe uma clara ligação com os objetivos de negócios. Processos de mensuração surgem mas não são consistentemente aplicados. Idéias relacionadas a um balanced scorecard de TI são adotadas, como a aplicação intuitiva de análise de causa de problemas.
4 Existe um entendimento de todos os requerimentos. Técnicas de comunicação maduras são aplicadas e ferramentas de comunicação padrão são utilizadas.	O processo é sólido e completo; boas práticas internas são aplicadas. Todos aspectos do processo são documentados e repetíveis. Políticas foram aprovadas e assinadas pela gerencia. Padrões para desenvolvimento e manutenção de processos e procedimentos são adotados e seguidos.	Ferramentas são implementadas de acordo com um plano padrão e algumas foram integradas com outras ferramentas relacionadas. Ferramentas são usadas nas principais áreas para automatizar o gerenciamento de processos e monitoramento de atividades e controles críticos.	Habilidades requeridas para todas as áreas são rotineiramente atualizadas, capacitação é assegurada para todas áreas críticas e certificações são encorajadas. Técnicas de treinamento maduras são aplicadas de acordo com o planejado e o compartilhamento de informação é encorajado. Todos especialistas internos são envolvidos e a efetividade do plano de treinamento é avaliada.	A responsabilidade e responsabilização são aceitas e funcionam de uma forma que habilita os proprietários de processos a executarem suas responsabilidades. A cultura de recompensas em uso motiva ações positivas.	Eficiência e efetividade são medidas e comunicadas, ligadas com os objetivos de negócios e com o plano estratégico de TI. O balanced scorecard de TI foi implementado em algumas áreas com exceções observadas pela gerencia e análises de causas de problemas são padronizadas. O aprimoramento contínuo está surgindo.
5 Existe um entendimento avançado dos requerimentos. Existe uma comunicação proativa das questões baseado em tendências, técnicas de comunicação maduras são aplicadas e ferramentas integradas são utilizadas.	Boas práticas externas e padrões são aplicadas. A documentação de processos evoluiu para ferramentas automatizadas de trabalho. Processos, políticas e procedimentos são padronizados e integrados para possibilitar o gerenciamento e aprimoramento.	Um conjunto de ferramentas padronizadas são usadas em toda empresa. Ferramentas são totalmente integradas com outras ferramentas integradas para suportar os processos de maneira completa. Ferramentas são usadas para suportar o aprimoramento do processo e automaticamente detectar exceções dos controles.	A organização formalmente encoraja a melhoria contínua de habilidades, baseado numa clara definição dos objetivos pessoais e organizacionais. Boas práticas externas para treinamento e educação são usadas, bem como conceitos e técnicas de ponta. O compartilhamento do conhecimento é uma cultura da empresa e sistemas baseados em conhecimento estão sendo entregues. Especialistas externos e líderes de mercado são utilizados para orientação.	Proprietários de processos recebem poder necessário para fazer decisões e agir. A aceitação da responsabilidade foi cascateada na inteira organização de uma maneira consistente.	Existe um sistema de mensuração de performance integrado ligando a performance de TI com os objetivos de negócio, através da aplicação geral do *balanced scorecard* de TI. Exceções são ampla e consistentemente observadas pela gerência e a análise de causa de problemas é aplicada. Contínua melhoria é um modo de vida.

Os objetivos são definidos de cima para baixo de maneira que os objetivos de negócios determinarão vários objetivos de TI que irão suportá-los. Um objetivo de TI é atingido através de um processo ou por interação de um determinado número de processos. Portanto, os objetivos de TI ajudam em diferentes objetivos de processos. Por sua vez, cada objetivo de processo requer um determinado número de atividades estabelecendo assim os objetivos da atividade. A figura 16 fornece um exemplo do relacionamento dos objetivos de negócios, TI, processos e atividades.

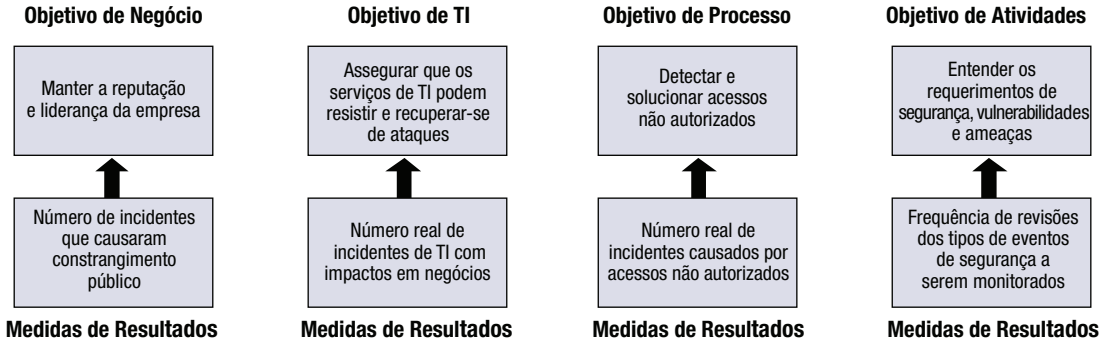
Figura 16 - Exemplo de Relacionamento de Objetivos



Os termos KGI e KPI usados em versões prévias do CobiT foram trocados por 2 tipos de métricas:

- Medidas de resultados (saídas), anteriormente indicadores-chaves de objetivos (KGIs), indicam se os objetivos foram atingidos. Esses podem ser medidos somente após os fatos e portanto são chamados de indicadores históricos *(lag indicators)*.
- Indicadores de performance, anteriormente indicadores-chaves de performance (KPIs), indicam se os objetivos serão possivelmente atingidos. Eles são medidos antes que os resultados sejam claros e portanto são chamados de indicadores futuros *(lead indicators)*.

Figura 17 - Possível Medida do Resultado para o Exemplo na Figura 16



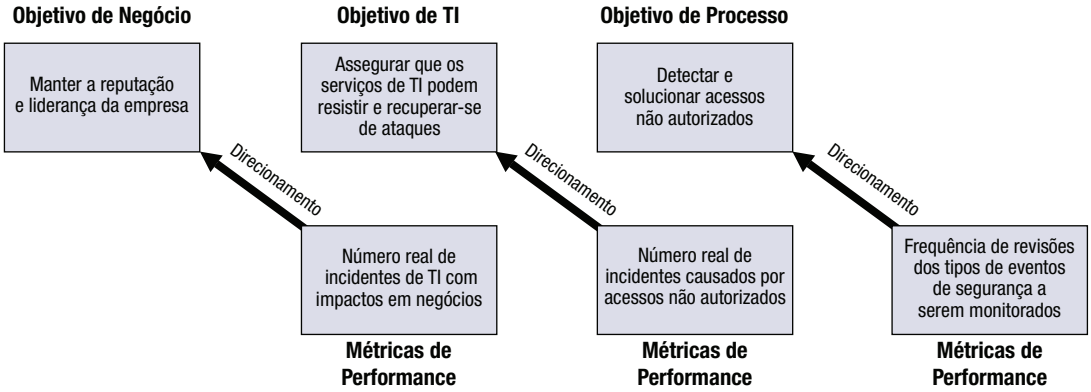
As medidas de resultados no nível menor tornam-se indicadores de performance para o nível maior. Como exemplificado na figura 16, uma medida de resultado indicando que a detecção e a solução de um acesso não autorizado estão nas metas irá também indicar que muito provavelmente os serviços de TI podem resistir a ataques e se recuperar deles. As medidas de resultados tornam-se um indicador de performance para o objetivo de nível superior. A Figura 18 ilustra como as medidas de resultados do exemplo tornam-se métricas de performance.

As medidas de resultados obtidas definem as medições que informam a gerência, depois dos fatos, se a função, os processos e a atividade de TI atingiram seus objetivos. Os medidores de resultados de funções de TI às vezes são expressos em termos de critérios de informação:

- Disponibilidade da informação necessária para suportar as necessidades de negócios
- Ausência de riscos de integridade e confidencialidade
- Eficiência de custos de processos e operação
- Confirmação de fidedignidade, efetividade e conformidade

Os indicadores de performance definem as medidas que determinam quão bem negócios, função de TI ou processo de TI estão sendo executados para permitir que os objetivos sejam atingidos. Eles são indicadores futuros ,*"lead indicators"*, quanto a se os objetivos serão atingidos, direcionando portanto os objetivos de maior nível. Eles às vezes medem a disponibilidade de apropriadas capacidades, práticas e habilidades, bem como os resultados de atividades relacionadas. Por exemplo, um serviço entregue por TI é um objetivo para TI mas é um indicador de performance e de capacidade para o negócio. É por isso que os indicadores de performance às vezes são chamados de direcionadores de performance, particularmente nos *"balanced scorecards"*.

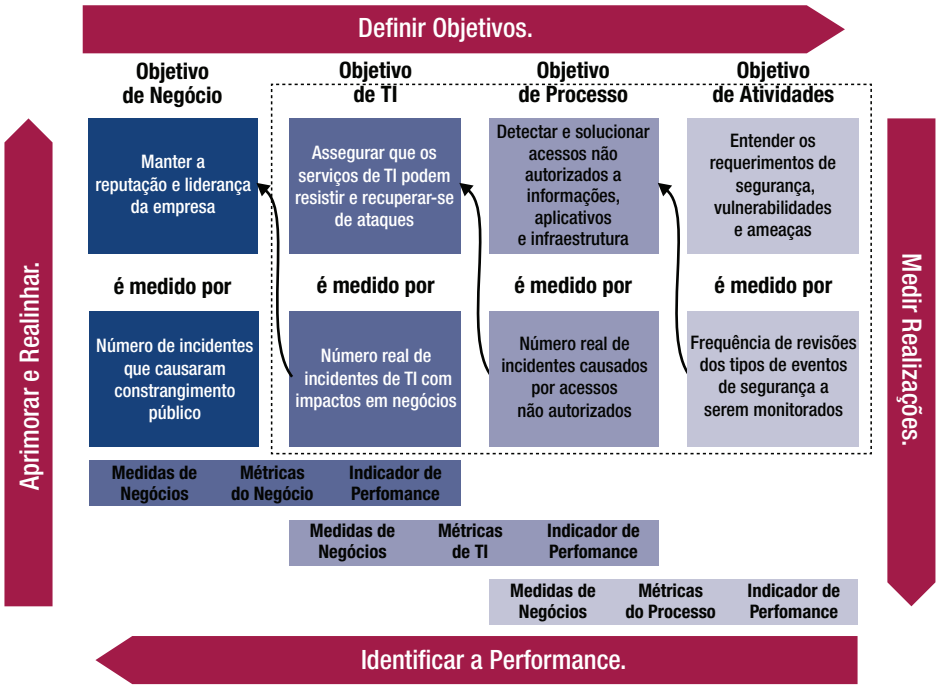
Figura 18 - Possíveis Direcionadores de Performance para o Exemplo na Figura 16



Portanto as métricas providas são tanto uma medida de resultados obtidos de uma função de TI, processo ou atividade de TI que elas medem, quando um indicador de performance direcionando um objetivo de maior nível de negócios, função de TI ou processo de TI.

A **Figura 19** ilustra o relacionamento entre os objetivos de negócios, TI, processos e atividades e suas diferentes métricas. Do canto superior esquerdo ao canto superior direito, são ilustrados os objetivos em cascata. Abaixo do objetivo está demonstrada a medida de resultados. As setas menores mostram que a mesma métrica é um indicador de performance para um objetivo de maior nível.

Figura 19 - Relacionamento entre Processos, Objetivos e Métricas (DS5)



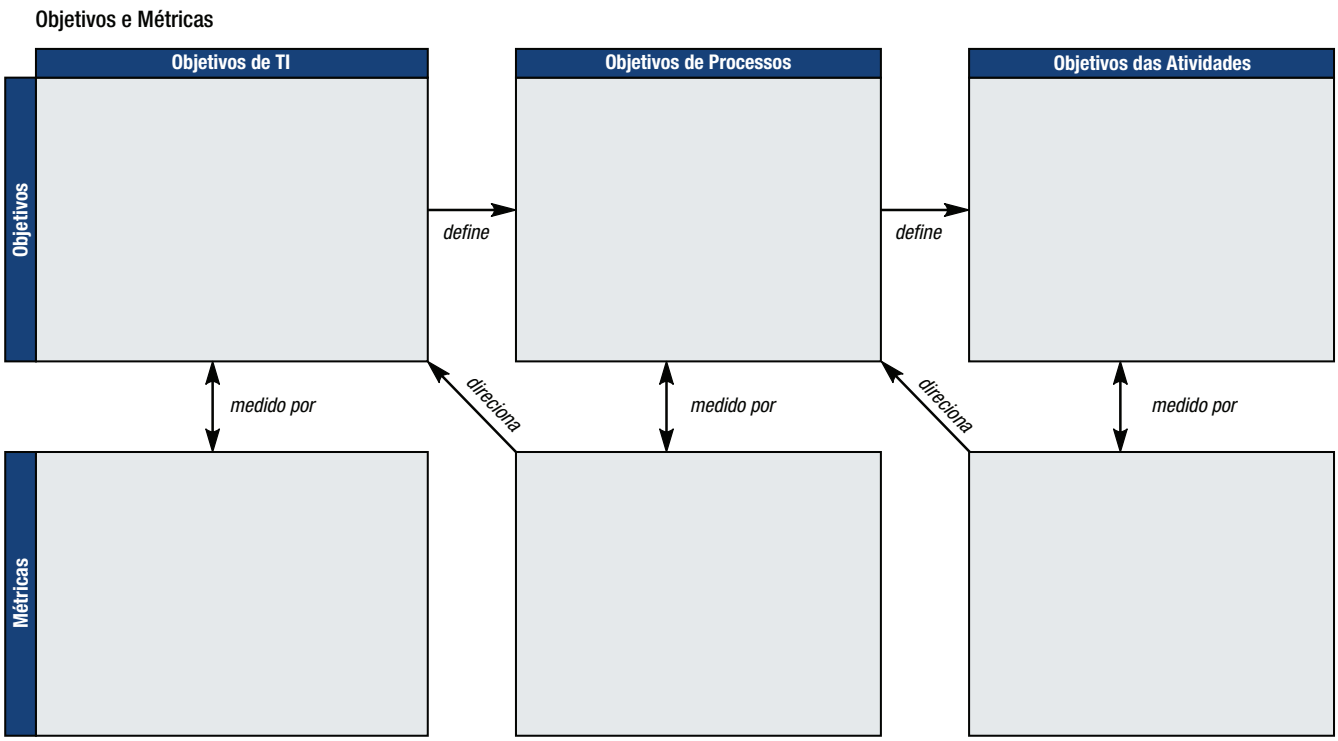
O exemplo acima provem do DS5 Garantir a segurança dos serviços. O CobiT oferece métricas somente para os resultados obtidos dos objetivos de TI como delineado pelas linhas tracejadas. Embora eles também são indicadores de performance de TI para os objetivos de negócios, o CobiT não fornece medidas de resultados para objetivos de negócios.

Os objetivos de negócios e de TI usados na seção de objetivos e métricas do CobiT, incluindo o seu relacionamento, são apresentados no Apêndice I. Para cada processo de TI no CobiT os objetivos e métricas são apresentados como indicado na figura 20.

As métricas foram desenvolvidas com as seguintes características em mente:

- Um índice elevado de preocupação com resultados versus o esforço (i.e., atenção na performance e em atingir os objetivos quando comparado com o esforço para capturá-los)
- Internamente comparável (i.e. um percentual de uma base ou números no tempo)
- Comparável externamente independente do tamanho da empresa ou mercado de atuação
- É melhor ter algumas boas métricas (pode até ser uma muito boa que poderia ser influenciada por diferentes meios) do que uma longa lista de métricas de baixa qualidade.
- Fácil de mensurar, não sendo confundida com metas

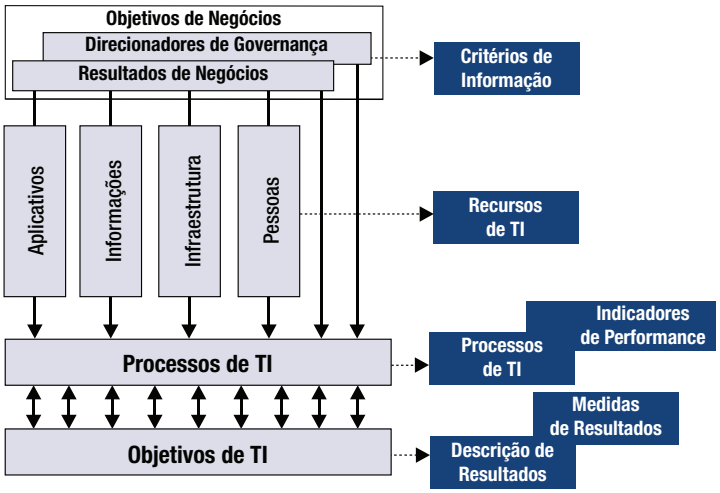
Figura 20 - Apresentação dos Objetivos e Métricas



A Estrutura do modelo CobiT

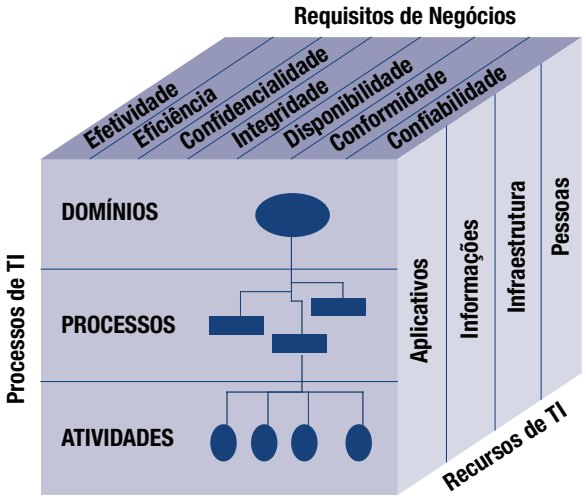
O modelo CobiT une os requisitos de negócios para informação e governança aos objetivos da função de serviços de TI. O modelo de processos do CobiT permite que as atividades de TI e os recursos que as suportam sejam serem apropriadamente gerenciados e controlados com base nos objetivos de controle de CobiT, bem como alinhados e monitorados usando os objetivos e métricas do CobiT, como ilustrado na **Figura 21**.

Figura 21 - Gerenciamento, Controle, Alinhamento e Monitoramento do CobiT



Em resumo, os recursos de TI são gerenciados pelos processos de TI para atingir os objetivos de TI que respondem aos requisitos de negócios. Este é o princípio básico do modelo CobiT, como ilustrado pelo cubo do CobiT (**Figura 22**).

Figura 22 - Figura do COBIT



Em maiores detalhes, todo o modelo COBIT pode ser mostrada graficamente como demonstrado na **figura 23**, com o modelo de processos do COBIT de 4 domínios contendo 34 processos genéricos, gerenciando os recursos de TI para entregarem as informações para a área de negócios de acordo com os requerimentos de negócios e governança.

Aceitabilidade Geral do COBIT

O COBIT é baseado na análise e na harmonização dos padrões e boas práticas de TI existentes, adequando-se aos princípios de governança geralmente aceitos. Ele está posicionado em alto nível, direcionado por requisitos de negócios, abrange todas as atividades de TI e concentra-se no *que* deveria ser obtido e não em *como* atingir uma efetiva governança, gerenciamento e controle. Sendo assim, ele age como um integrador das práticas de governança de TI e influencia a Alta Direção, gerências de negócios e de TI, profissionais de governança, avaliação e segurança, profissionais de auditoria de TI e de controles. Ele é desenhado para ser complementar e utilizado com outros padrões e boas práticas.

A implementação de boas práticas deve ser consistente com a governança e o ambiente de controle da organização, apropriado para a organização e integrada a outros métodos e práticas utilizadas. Padrões e boas práticas não são uma panacéia. Sua efetividade depende d como foram implementados e mantidos atualizados. Eles são mais úteis quando aplicados como um conjunto de princípios e um ponto de partida para produzir procedimentos específicos. Para evitar que as práticas fiquem só no papel, a gerência e os funcionários devem entender o que fazer, como fazer e porque isso é importante.

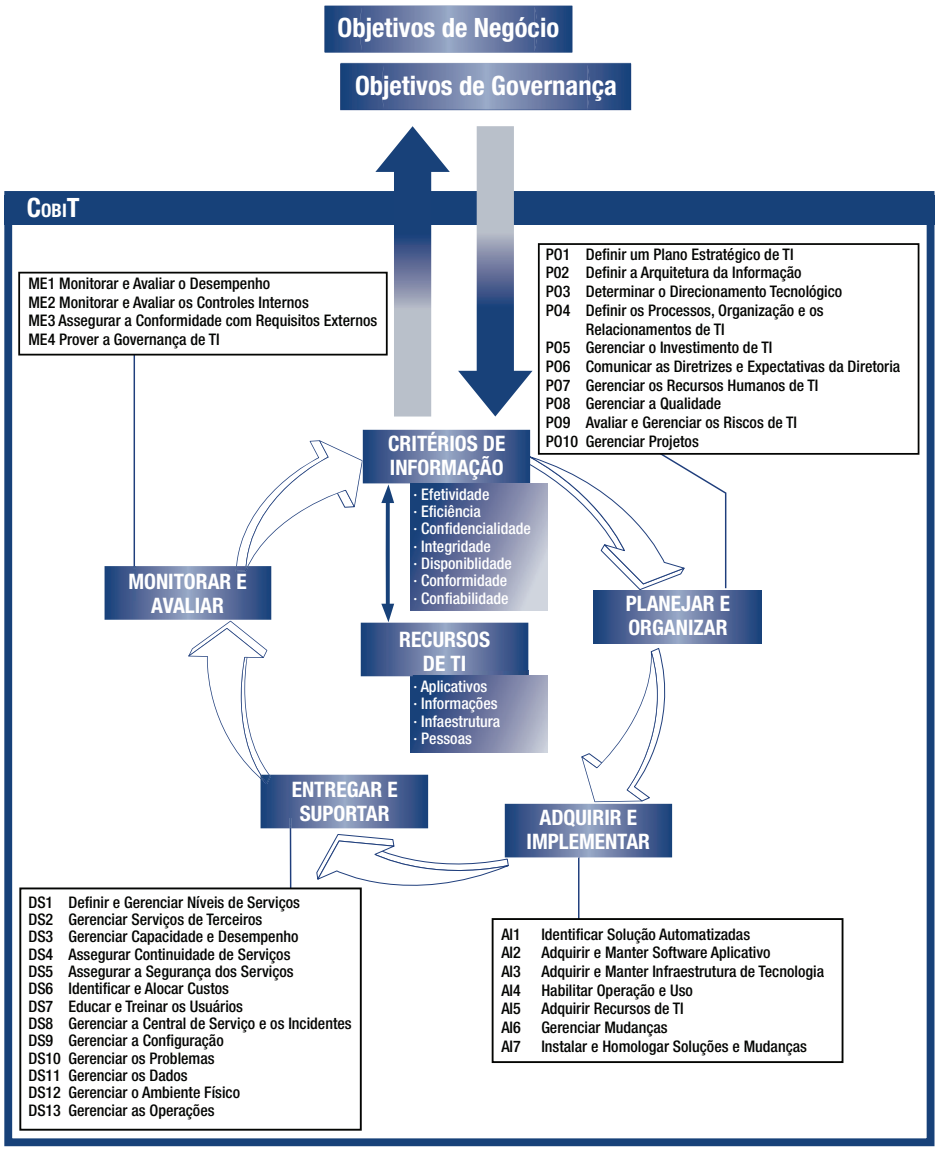
Para atingir o alinhamento das boas práticas com os requisitos de negócios é recomendável que o COBIT seja utilizado num alto nível, provendo uma metodologia de controle geral com base em um modelo de processos de TI que deve servir genericamente para toda empresa. Práticas específicas e padrões cobrindo áreas específicas podem ser mapeados com a metodologia COBIT, provendo assim um material de orientação.

O COBIT influencia diferentes usuários:
- **Alta Direção:** Para obter valor dos investimentos de TI, balancear os riscos e controlar o investimento em um ambiente de TI às vezes imprevisível
- **Executivos de negócios:** Para assegurar que o gerenciamento e o controle dos serviços de TI oferecidos internamente e por terceiros estejam funcionando de modo adequado
- **Executivos de TI:** Para prover os serviços de TI de que o negócio precisa para suportar a estratégia de negócios de maneira controlada e gerenciada
- **Auditores:** Para substanciar suas opiniões e/ou prover recomendações sobre controles internos para os executivos

O COBIT foi desenvolvido e é mantido por um instituto de pesquisa independente e sem fins lucrativos, contando com a experiência de seus membros associados, especialistas e profissionais de controle e segurança. O seu conteúdo baseia-se em uma contínua pesquisa das boas práticas de TI e é atualizado continuamente, provendo um recurso objetivo e prático para todos os tipos de usuários.

O COBIT é orientado para os objetivos e escopo da governança de TI, assegurando que a metodologia de controle seja compreensiva, alinhada com os princípios de governança de organizações e, portanto, aceitável para Alta Direção, executivos, auditores e reguladores. Um mapa demonstrando como os objetivos de controles do COBIT são mapeados com as cinco áreas de foco da governança de TI e das atividades de controle do COSO é demonstrado no Apêndice II.

Figura 23 - Visão Geral do Modelo do CobiT



A **Figura 24** resume como os vários elementos do modelo CobiT podem ser mapeados com as áreas de foco de governança de TI.

Figura 24 - Modelo CobiT e as Áreas Foco da Governança de TI

	Objetivos	Métricas	Práticas	Modelos de Maturidade
Alinhamento Estratégico	P	P		
Entrega de Valor		P	S	P
Gerenciamento de Risco		S	P	S
Gerenciamento de Recursos		S	P	P
Gerenciamento de Performance	P	P		S

P = Ferramenta Primária S = Ferramenta Secundária

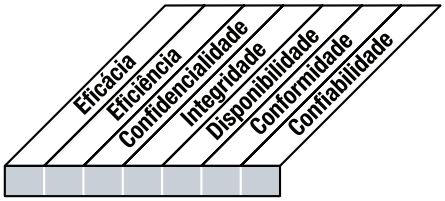
COMO UTILIZAR ESTE LIVRO

Navegação pelo Modelo COBIT

Para cada um dos processos de TI do COBIT é apresentado uma descrição em conjunto com os principais objetivos e métricas no formato de cascata (**Figura 25**).

Figura 25 - Navegação COBIT

Em cada processo de TI, são fornecidos objetivos de controle como declarações de ações genéricas com o mínimo de boas práticas gerenciais para garantir que o processo esteja mantido sob controle.



Controle sobre o seguinte processo de TI:

Nome do processo

que satisfaça aos seguintes requisitos do negócio para a TI:

sumário do objetivo de TI mais importante

com foco em:

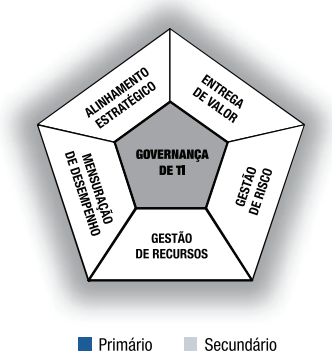
sumário dos objetivos de processos mais importantes

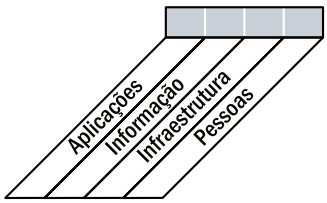
é alcançado por:

objetivos da atividade

e medido por:

métricas chaves





Visão Geral dos Principais Componentes do COBIT

O modelo COBIT é formado pelos seguintes componentes principais, apresentados no restante desta publicação e organizado por 34 processos de TI, mostrando uma visão geral de como controlar, gerenciar e mensurar cada processo. Cada processo é coberto por quatro seções e cada uma delas é apresentada em cerca de uma página, como segue:

- A seção 1 **(Figura 25)** contém uma descrição do processo que resume os objetivos do processo, apresentada no formato de cascata. Esta página também demonstra o mapeamento dos critérios de informação, recursos de TI e áreas de foco de governança de TI. A letra P indica um relacionamento primário e a letra S indica um secundário.
- A seção 2 apresenta os objetivos de controle desse processo.
- A seção 3 apresenta os processos de entrada e saída, tabela RACI, objetivos e métricas.
- A seção 4 apresenta o modelo de maturidade do processo.

Outro modo de visualizar a performance do processo é avaliar se:
· As entradas do processo são o que o proprietário do processo precisa dos outros.
· A descrição dos objetivos de controle do processo define o que o proprietário do processo deve fazer.
· As saídas do processo são aquelas que o proprietário do processo tem que entregar.
· Os objetivos e métricas demonstram como o processo deve ser medido.
· A tabela RACI define o que precisa ser delegado e para quem.
· O modelo de maturidade demonstra o que precisa ser feito para o aprimoramento.

As responsabilidades na tabela RACI são categorizadas para todos os processos, como segue:
· *Chief executive officer* (CEO)
· *Chief financial officer* (CFO)
· Executivo de Negócio
· *Chief information officer* (CIO)
· Proprietário do Processo de Negócio
· Chefe de Operações
· Responsável por Arquitetura
· Responsável por Desenvolvimento
· Responsável pela Administração de TI (nas grandes empresas, é o responsável por funções como recursos humanos, orçamentos e controles internos)
· *Project management officer* (PMO) ou função equivalente
· Conformidade, auditoria, riscos e segurança (grupos como responsabilidades por controles mas não de operações de TI)

Certos processos têm papéis especializados específicos do processo, por exemplo, gerenciar a central de serviços e os incidentes do DS8.

Deve ser observado que embora o material tenha sido coletado de centenas de especialistas, seguindo rigorosa pesquisa e revisão, as entradas, as saídas, as responsabilidades, as métricas e os objetivos são ilustrativos e não uma receita completa ou exaustiva. Eles fornecem uma base de conhecimento especializado a partir da qual cada organização deve selecionar o que se aplica de maneira eficiente e eficaz considerando-se a estratégia, os objetivos e as políticas da organização.

Os Usuários dos Componentes do CobiT

A gerência pode utilizar o material CobiT para avaliar os processos de TI usando as metas de negócios e as metas de TI detalhadas no Apêndice I para visando esclarecer dos processos de TI e os modelos de maturidade de processo para avaliar a performance atual.

Responsáveis pela implementação e auditores podem identificar os requisitos de controle aplicáveis a partir dos objetivos de controles e das responsabilidades pelas atividades apresentadas na tabela RACI associada.

Todos os usuários em potencial podem se beneficiar da utilização do conteúdo do CobiT como um enfoque geral para o gerenciamento e governança de TI em conjunto com os seguintes padrões mais detalhados:
· ITIL para entrega de serviços
· CMM para entrega de soluções
· ISO 17799 para segurança da informação
· PMBOK ou PRINCE2 para gerenciamento de projetos

Apêndices

As seguintes seções adicionais de referência estão disponíveis no final deste livro:
I. Tabelas Relacionando os Objetivos e Processos (três tabelas)
II. Mapeamento dos Processos de TI com as Áreas Foco de Governança de TI, COSO, Recursos de TI do CobiT e Critérios de Informação do CobiT
III. Modelo de Maturidade para Controles Internos
IV. Material de Referência Principal do CobiT
V. Referência cruzada entre a 3ª edição do CobiT e o CobiT 4.1
VI. Enfoque de Pesquisa e Desenvolvimento
VII. Glossário
VIII. O CobiT e os Produtos Relacionados