Processos de TI do COBIT 4.1

PLANEJAMENTO E ORGANIZAÇÃO

PO1 Definir um Plano Estratégico de TI

O planejamento estratégico é requerido para gerenciar e direcionar todos os recursos da TI em linha com as estratégias e prioridades do negócio. A função da TI e os stakeholder's do negócio são responsáveis para assegurar que um valor otimizado é realizado através dos portfolios dos projetos e serviços. O plano estratégico deve aumentar a compreensão dos stakeholder's chaves em relação das oportunidades e limites da TI, avaliar o desempenho atual e esclarecer o nível de investimentos requeridos. A estratégia e as prioridades do negócio devem ser refletidas nos portfolios e executadas através dos planos táticos da TI, os quais estabeleçam objetivos concisos, planos e tarefas compreendidas e aceitos pelo negócio e da TI.

PO2 Definir a Arquitetura de Informação

A função dos sistemas de informação deve criar e atualizar regularmente um modelo de informação de negócio e definir os sistemas apropriados para otimizar o uso da informação. Isso inclua o desenvolvimento de um dicionário coorporativo de dados com as regras de sintaxe da organização, esquema de classificação de dados e níveis de segurança. Este processo melhora a qualidade de decisões feitas pelas gerencias e assegura que informações confiáveis e seguras são providas e isso habilita de racionalizar recursos de sistemas de informação para atender apropriadamente as estratégias de negócio. Este processo da TI também necessita de aumentar a responsabilidade sobre a integridade e segurança dos dados e melhorar a efetividade e controle sobre o compartilhamento de informação através de aplicações e entidades.

PO3 Determinar a Direção Tecnológica

A função dos serviços de informação deve determinar a direção tecnológica para suportar o negócio. Isso requer a criação de um plano da infra-estrutura tecnológica e um comitê de arquitetura que fixa e gerencia expectativas claras e realísticas o que a tecnologia pode oferecer em termos de produtos, serviços e mecanismos de entrega. O plano deve ser atualizado regularmente e incluir aspectos como a arquitetura de sistemas, direção tecnológica, planos de aquisição, padrões, estratégias de migração e contingência. Isso habilita uma resposta em tempo para mudar para um ambiente competitiva, economias em escala com o pessoal e os investimentos em sistemas de informação e um investimento que melhora a interoperabilidade de plataformas e aplicações.

PO4 Definir Processos de TI, Organização e Relacionamento

Uma organização da TI precisa ser definida, considerando os requerimentos para pessoas, habilidades, funções, responsabilidade, autoridade, papeis e supervisão. Esta organização deve estar embutida dentro um framework de processos da TI que asseguram transparência e controle, como também envolvem os executivos sênior e gerentes de negócio. Um comitê estratégico deve assegurar uma visão geral da TI e um ou mais comitês de direção, em quais os participantes do negócio e da TI devem determinar a priorização dos recursos da TI em linha com as necessidades do negócio. Processos, políticas e procedimentos administrativos necessitam de ser implementadas para todas as funções, com atenção especifica para o controle, garantia de qualidade, gerenciamento de riscos, segurança de informação, propriedade para dados e sistemas e segregação de direitos. Para assegurar um suporte em tempo para os requerimentos do negócio, a TI deve estar envolvida em processos relevantes de decisão.

PO5 Gerenciar o Investimento em TI

Estabelecer e manter um framework para gerenciar programas que habilitem investimentos em TI e que abrangem custos, benefícios, priorização nos orçamentos, um processo formal de orçamentos e gerenciamento em relação dos orçamentos. Trabalhar com os stakeholder's para identificar e controlar o total dos custos e benefícios dentro do contexto dos planos estratégicos e táticos da TI e iniciar ações corretivas quando necessárias. O processo deve favorecer os relacionamentos entre a TI e stakeholder's do negócio, habilitar o uso efetivo e eficiente dos recursos da TI e prover transparência e responsabilidade nos custos totais de propriedade, a relação do beneficio para o negócio e o retorno sobre investimentos que habilitam a TI.

PO6 Comunicar Metas e Diretivas Gerenciais

A administração deve desenvolver um framework de controle empresarial da TI e definir e comunicar políticas. Um programa continua de comunicação deve ser implementada para articular a missão, objetivos de serviço, políticas e procedimentos, etc. aprovados e suportados pela administração. A comunicação suporta o atingimento dos objetivos da TI e assegura conscientização e compreensão em relação do negócio e os riscos, objetivos e a direção da TI. O processo deve assegurar a conformidade com leis e regulamentos.

PO7 Gerenciar Recursos Humanos

Adquire, mantêm e motiva uma força de trabalho competente para criar e entregar serviços da Ti para o negócio. Isso é atingido seguindo praticas definidos e acordadas que suportam o recrutamento, treinamento, avaliação do desempenho, promoção e demissão. Este processo é critico, como as pessoas são um ativo e de governança importante e o ambiente interno de controle depende bastante da motivação e competência do pessoal.

PO8 Gerenciar Qualidade

Um sistema de gerenciamento da qualidade deve ser desenvolvido e mantido, o qual inclua um processo de desenvolvimento e aquisição comprovado e padronizado. Isso é habilitado através do planejamento, implementação e manutenção do sistema de qualidade que provêm requerimentos claros de qualidade, procedimentos e políticas. Requerimentos de qualidade devem ser determinados e comunicados, com indicadores quantificáveis e atingíveis. Melhorias contínuas são atingidas através de um monitoramento operacional, analises e ações sobre desvios e a comunicação dos resultados para os stakeholder's. Gerenciamento da qualidade é essencial para assegurar que a TI entrega valor para o negócio, melhorias contínuas e transparência para stakeholder's.

PO9 Avaliar e Gerenciar Riscos

Criar e manter um framework de gerenciamento de riscos. O framework documenta um nível de riscos da TI comum e acordado, estratégias de mitigação e acordos sobre riscos residuais. Qualquer impacto potencial sobre as metas da organização, causada por eventos não planejados, deve ser identificado, levantado e avaliado. Estratégias de mitigação de riscos devem ser adotadas para minimizar riscos residuais ao um nível aceitável. O resultado da avaliação deve ser compreensível para os stakeholder's e expresso em termos financeiros, para habilitar os stakeholder's de alinhar os riscos com um nível aceitável de tolerância.

PO10 Gerenciar Projetos

Estabelecer um framework de gerenciamento de programas e projetos para gerenciar todos os projetos da TI. Este framework deve assegurar a correta priorização e coordenação de todos os projetos. O framework deve incluir um plano mestre, atribuição de recursos, definição de entregáveis, aprovações pelos usuários, uma abordagem em fases para as entregáveis, garantia de qualidade, um plano formal de teste, testes e revisões pós-implementação após da instalação para assegurar o gerenciamento de risco e a entrega do valor para o negócio. Esta abordagem reduz o risco de custos não esperados e cancelamento de projetos, aumenta a comunicação com os envolvidos do negócio e usuários finais, assegura o valor e a qualidade dos entregáveis do projeto e maximiza a contribuição de programas que habilitam investimentos em TI.

AQUISIÇÃO E IMPLEMENTAÇÃO

AI1 Identificar soluções automatizadas

A necessidade para novas aplicações ou funções requer uma análise antes da aquisição ou criação para assegurar que os requerimentos do negócio são satisfeitos numa abordagem efetiva e eficiente. Este processo cubra a definição das necessidades, considerando fontes alternativas, revisão da viabilidade tecnológica e econômica, execução de análise de risco e análise de custo / beneficio e a conclusão de uma decisão final de "fazer" ou "comprar". Todos estes passos habilitam a organização de minimizar os custos de adquirir e implementar soluções, enquanto asseguram que estes habilitam o negócio de atingir seus objetivos.

AI2 Adquirir e manter software aplicativo

Aplicações devem estar disponíveis em linha com os requerimentos de negócio. Este processo envolve o desenho de aplicações, a inclusão apropriada de controles de aplicação e requerimentos de segurança e o atual desenvolvimento e configuração conforme os padrões. Isso permita as organizações de suportar apropriadamente as operações de negócio com as corretas aplicações automatizadas.

AI3 Adquirir e manter arquitetura tecnológica

Organizações devem haver um processo para a aquisição, implementação e atualização da infra-estrutura tecnológica. Isso requer uma abordagem planejada para a aquisição, manutenção e proteção da infra-estrutura em linha com as estratégias tecnológicas acordadas e a provisão de ambientes de desenvolvimento e teste. Isso assegura que o suporte tecnológico operacional suporta as aplicações de negócio.

AI4 Manter operação e uso

Conhecimento sobre novos sistemas necessita de ser disponibilizado. Este processo requer a produção de documentação e manuais para usuários e TI e prover treinamento que assegura o uso e a operação apropriado de aplicações e infra-estrutura.

AI5 Obter Recursos de TI

Recursos de TI, inclusive pessoas, hardware, software e serviços, necessitam ser obtidos. Isso requer uma definição e sanção de procedimentos de aquisição, a seleção de fornecedores, a realização de arranjos contratuais e a aquisição em se. Fazer assim assegura que a organização tem todos os recursos de TI requeridos em tempo e de maneira efetivo em custo.

AI6 Gerenciar mudanças

Todas as mudanças, inclusive mudanças emergenciais e correções, relacionados à infra-estrutura e aplicações dentro de um ambiente de produção precisam ser gerenciados formalmente de uma maneira controlada. Mudanças (incluindo procedimentos,

processos, sistemas e parâmetros de serviços) precisam ser registradas, avaliados e autorizadas antes de implementar e revisados em relação dos resultados planejados em seguida da implementação. Isso assegura a mitigação de riscos de impactos negativos sobre a estabilidade ou integridade de ambientes produtivos.

AI7 Instalar e certificar Soluções e Mudanças

Novos sistemas precisam ser feitos operacionais uma vez que o desenvolvimento é completo. Isso requer testes apropriados em um ambiente dedicado com dados de teste relevantes, definição da introdução e instruções de migração, planejamento de liberações, promoção atual para a produção e revisões pós-implementação. Isso assegura que sistemas operacionais estão em linha com as expectativas e resultados acordados.

ENTREGA E SUPORTE

DS1 Definir níveis de Serviços

Comunicação efetiva entre a gerência da TI e os clientes do negócio, em relação dos serviços requeridos, é habilitado através da documentação e o acordo de serviços da TI e níveis de serviços. Este processo também inclua o monitoramento e o reporte em tempo para os stakeholders sobre o cumprimento dos níveis de serviços. Este processo habilita o alinhamento entre os serviços da TI o os requerimentos de negócio associados.

DS2 Gerenciar Serviços de Terceiros

A necessidade de assegurar que serviços providos por terceiros atendem os requerimentos do negócio requer um processo efetivo de gerenciamento de terceiros. Este processo é efetuado com papeis claramente definidos, responsabilidades e expectativas em acordos com terceiros, como também com revisão e monitoramento destes acordos para efetividade e conformidade. Gerenciamento efetivo de serviços de terceiros minimiza os riscos de negócio associados com fornecedores não conformes.

DS3 Gerenciar Performance e Capacidade

A necessidade de gerenciar o desempenho e a capacidades dos recursos de TI requer um processo para rever periodicamente o desempenho e a capacidade atual dos recursos da TI. Este processo inclua a previsão das futuras necessidades baseada na carga de trabalho, requerimentos de armazenamento e de contingência. Este processo provém a garantia que os recursos da informática, que suportam os requerimentos de negócio, são continuamente avaliados.

DS4 Garantir Continuidade dos Serviços

A necessidade de prover serviços contínuos de TI requer o desenvolvimento, manutenção e testes de planos de continuidade da TI, armazenamento externo de backup e treinamento periódico para o plano de continuidade. Um processo efetivo da continuidade de serviço minimiza a probabilidade e o impacto de interrupções maiores de serviço sobre funções e processos de negócio.

DS5 Garantir Segurança dos Sistemas

A necessidade de manter a integridade da informação e proteger os ativos da TI requer um processo de gerenciamento de segurança. Este processo inclui de estabelecer e manter papeis e responsabilidades, políticas, padrões e procedimentos da segurança de TI. Gerenciamento da segurança também inclui realizar monitoramento da segurança, testes periódicos e implementar ações corretivas para identificar fraquezas ou incidentes de segurança. Um gerenciamento efetivo de segurança proteja todos os ativos da TI para minimizar o impacto sobre o negócio das vulnerabilidades e incidentes de segurança.

DS6 Identificar e Alocar Custos

A necessidade para um justo e imparcial sistema de alocar custos para o negócio requer a medição exata de custos da TI e acordos com usuários de negócio para uma alocação correta. Este processo inclua a criação e operação de um sistema de captura, alocação e reporte dos custos da TI para os usuários de serviços. Um sistema justo de alocação habilita o negócio de fazer mais decisões informadas em relação do uso de serviços da TI.

DS7 Educar e Treinar usuários

Educação efetiva de todos os usuários de sistemas de TI, incluindo estes dentro da TI, requer a identificação das necessidades de treinamento de cada grupo de usuários. Em adição da identificação da necessidade, este processo inclua a definição e execução de uma estratégia para um treinamento efetivo e medição de resultados. Um programa efetivo de treinamento aumenta o uso efetivo da tecnologia com a redução de erros de usuários, aumenta a produtividade e aumenta a conformidade com controles chaves como as medidas de segurança de usuários.

DS8 Gerenciar Service Desk e Incidentes

Respostas em tempo e efetivos para as perguntas e problemas dos usuários da TI requerem uma central de serviço bem desenhada e implementada e um processo de gerenciamento de incidentes. Este processo inclua a implementação da função da central de serviços com registro, escalação, tendências, análise de causas raiz e resolução de incidentes. O benefício para o negócio inclua um

aumento de produtividade através da resolução rápido das perguntas dos usuários. Em adição, o negócio pode endereçar causas raiz (como um pobre treinamento de usuários) através de um reporte efetivo.

DS9 Gerenciar a Configuração

Assegurar a integridade da configuração de hardware e software requer de estabelecer e manter um preciso e completo repositório da configuração. Este processo inclua a coleta inicial de informação da configuração, estabelecer referências, verificar e auditar a informação da configuração e atualizar o repositório da configuração quando necessário. Gerenciamento efetivo da configuração facilita a disponibilidade maior do sistema, minimizar assuntos de produção e resolver estes assuntos mais rápidos.

DS10 Gerenciar Problemas

Um gerenciamento efetivo de problemas requer a identificação e classificação de problemas, análise da causa raiz e resolução de problemas. O processo do gerenciamento de problemas também inclua a identificação de recomendações para melhorar a manutenção de registros de problemas e revisar o status de ações corretivas. Um processo do gerenciamento de problemas efetivo melhora níveis de serviço, reduz custos e melhora a conveniência e satisfação.

DS11 Gerenciar Dados

Gerenciamento efetivo de dados requer a identificação de requerimentos para dados. O processo de gerenciamento de dados também inclua estabelecer procedimentos efetivos para gerenciar a biblioteca de mídias, backup e recuperação e disponibilizar mídias apropriadas. Gerenciamento efetivo de dados ajuda assegurar a qualidade, oportunidade e disponibilidade de dados do negócio.

DS12 Gerenciar os Ambientes Físicos

A proteção para equipamentos de computação e pessoal requer instalações bem desenhadas e bem gerenciadas. O processo de gerenciar o ambiente físico inclua de definir os requerimentos para um lugar físico, seleção de instalações apropriadas e desenho efetivo dos processos para monitorar elementos ambientais e gerenciar o acesso físico. Gerenciamento efetivo do ambiente físico reduz interrupções do negócio devida de danos nos equipamentos de computação e no pessoal.

DS13 Gerenciar Operações

Processamento completo e exato de dados requer o gerenciamento efetivo do processamento de dados e a manutenção de hardware. Este processo inclua a definição de políticas e procedimentos operacionais para um gerenciamento efetivo da programação do processamento, proteção de output sensitivo, monitoramento da infra-estrutura e manutenção preventiva de hardware. Gerenciamento efetivo da operação ajuda de manter a integridade de dados e reduz atrasos no negócio e custos da operação da TI.

MONITORAÇÃO E AVALIAÇÃO

ME1 Monitorar e Avaliar a Performance de TI

Assegura que a administração estabeleça um framework geral de monitoramento e uma abordagem que defina o escopo, metodologia e processos para serem seguidos para o monitoramento da TI contribua para os resultados do gerenciamento do portfolio empresarial e processos de programas gerenciais e estes processos que são específicos para entregar as competências e serviços da TI. O framework deve estar integrado com o sistema de gerenciamento de desempenho da companhia.

ME2 Monitorar e Avaliar Controle Interno

Estabelecer um programa de controle interno efetivo para a TI requer um processo de monitoração bem definido. Este processo inclui monitoração e reporte de exceções de controle, resultados da auto-avaliação e revisão de fornecedores (terceiros). Um benefício principal do controle interno de monitoração é fornecer segurança relacionada à eficiência e eficácia das operacionais e conformidade com leis e regulamentos.

ME3 Assegurar Conformidade Regulatória

Uma vigilância regulatória eficiente requer o estabelecimento de um processo de revisão independente para garantir a conformidade com leis e regulamentos. Este processo inclui definir um auditor independente, ética profissional e padrões, planejamento, desempenho do trabalho de auditoria, e reporte do acompanhamento das atividades de auditoria. O propósito deste processo é fornecer uma garantia positiva relacionada à conformidade da TI com leis e regulamentos.

ME4 Fornecer Governança de TI

Estabelecer um framework efetivo de governança, incluindo a definição de estruturas organizacionais, processos, liderança, papeis e responsabilidades para assegurar que os investimentos em TI empresarial são alinhados e entregas de acordo com as estratégias e objetivos empresariais.