Governança de TI

O termo “Governança de TI” tem suas origens no conceito de “Governança Corporativa”, mas não devemos confundir esses conceitos. Além disso, a "Governança de TI" relaciona-se com a "Gestão/gerenciamento de TI", porém não são a mesma coisa. Para melhor entendermos as semelhanças, as diferenças e o inter-relacionamento do significado desses termos, seguem algumas definições.

Governança Corporativa

Segundo o Instituto Brasileiro de Governança Corporativa (IBGC):

"Governança Corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, Conselho de Administração, Diretoria e órgãos de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso a recursos e contribuindo para sua longevidade."

Governança de TI

Para o Ministro Aroldo Cedraz, “Governança de TI é o conjunto estruturado de políticas, normas, métodos e procedimentos destinados a permitir à alta administração e aos executivos o planejamento, a direção e o controle da utilização atual e futura de tecnologia da informação, de modo a assegurar, a um nível aceitável de risco, eficiente utilização de recursos, apoio aos processos da organização e alinhamento estratégico com objetivos desta última. Seu objetivo, pois, é garantir que o uso da TI agregue valor ao negócio da organização.” (Voto do Ministro Relator – Acórdão 2.308/2010 – Plenário)

Para o Information Technology Governance Institute (ITGI), “governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização.”

Observa-se, portanto, que a “Governança Corporativa” tem foco no direcionamento e monitoramento da gestão da instituição, e busca permitir a intervenção dos responsáveis finais sempre que houver desvio em relação ao esperado. Em última instância, esses responsáveis são os detentores da propriedade: sócios e acionistas, no caso das organizações privadas, e a sociedade, no caso das organizações públicas federais.

Já a “Governança de TI” tem foco no direcionamento e monitoramento das práticas de gestão e uso da TI de uma organização, tendo como indutor e principal beneficiário a alta administração da instituição.

Um exemplo prático de mecanismo de governança de TI é o estabelecimento de um processo transparente de tomada de decisão sobre a priorização de grandes demandas de TI. Tal processo é necessário para garantir que as ações de TI estejam alinhadas com os objetivos institucionais e para garantir que as demandas que tenham maior impacto nesses objetivos tenham atendimento prioritário. Esta é uma decisão que não cabe às unidades de TI (embora devam sempre opinar). Portanto, o estabelecimento desse processo, os participantes e suas competências é uma iniciativa de governança de TI a ser liderada pela alta administração.

Gerenciamento ou Gestão de TI

Conjunto de processos realizados pelas unidades provedoras de TI, visando ao planejamento e à realização das atividades necessárias ao provimento ou entrega de soluções e serviços de TI.

Relação entre os Conceitos

Do que vimos, pode-se pensar, erroneamente, que a Governança Corporativa não tem relação com a Governança de TI e que esta não tem relação com a Gestão/Gerenciamento de TI. Entretanto, o que de fato ocorre é uma dependência entre elas, tal como mostrado na figura abaixo. O gerenciamento de serviços de TI é, de fato, um enabler (facilitador) da governança de TI e esta é um facilitador da governança corporativa.

Em resumo, uma organização que faça uso intenso de TI (situação comum, atualmente), não pode afirmar ter uma boa governança corporativa sem ter boa governança de TI. Igualmente, a instituição não pode afirmar ter uma boa governança de TI sem ter um bom gerenciamento de (serviços) de TI.

Áreas de Foco da Governança de TI

Na prática, a Governança de TI se traduz em um conjunto de políticas, processos, papéis e responsabilidades associados a estruturas e pessoas da organização, de modo a se estabelecer claramente o processo de tomada de decisões e as diretrizes para o gerenciamento e uso da TI, tudo isso de forma alinhada com a visão, missão e metas estratégicas da organização.

A figura abaixo resume as principais dimensões focalizadas pela Governança de TI.

Áreas de foco da Governança de TI Na prática, a Governança de TI se traduz em um conjunto de políticas, processos, papéis e responsabilidades associados a estruturas e pessoas da organização, de modo a se estabelecer claramente o processo de tomada de decisões e as diretrizes para o gerenciamento e uso da TI, tudo isso de forma alinhada com a visão, missão e metas estratégicas da organização.

Alinhamento Estratégico - assegura o alinhamento dos planos da TI com os de negócio e alinha a operação e as entregas da TI com as operações da organização.

Entrega de Valor – assegura que os benefícios previstos pela TI estão realmente sendo gerados, dentre eles a otimização de custos e outros valores intrínsecos que a TI pode proporcionar.

Gestão de Riscos – Permite que a organização reconheça todos os riscos (e oportunidades) derivados da TI para o negócio e que decida e tenha planos para mitigá-los na medida que julgue necessário.

Gestão de Recursos – assegura a gestão dos recursos mais importantes para TI: recursos humanos e recursos tecnológicos (informações, infraestrutura, aplicações). Promove a valorização do conhecimento e da infraestrutura.

Mensuração de Desempenho – acompanha e monitora a implementação da estratégia, consumação de projetos, uso dos recursos e entrega dos serviços quanto à sua contribuição para as estratégias e objetivos do negócio, utilizando-se não apenas de critérios financeiros.

Importância de se Aplicar Governança de TI no TCU

O TCU é uma instituição que depende de informação para a realização de seus trabalhos, e cada vez mais da Tecnologia da Informação (TI) para adequadamente tratar, analisar, fazer uso, disseminar e proteger essas informações. Além disso, é cada vez maior a automação de processos de trabalho do Tribunal, como meio de se assegurar o alcance e a manutenção de padrões de desempenho e qualidade compatíveis com as necessidades da sociedade brasileira.

Entretanto, não é suficiente simplesmente reconhecer a importância da TI e aplicar recursos e esforços em tais iniciativas. No mercado, são incontáveis os exemplos de projetos de TI que fracassaram pela falta ou imaturidade dos mecanismos de governança de TI.

Organizações bem-sucedidas reconhecem os benefícios da tecnologia da informação e a utilizam para adicionar valor ao negócio, valendo-se de mecanismos de governança de TI adequados às estratégias institucionais.

Para saber mais sobre os mecanismos de governança de TI atualmente utilizados no TCU, consulte a seção "Mecanismos de Governança de TI no TCU".

Entenda como a Governança de TI pode ajudar a sua empresa

Para aumentar a sua competitividade no mercado e garantir os melhores processos dentro de sua empresa, certamente você conta com diversas ferramentas de Tecnologia da Informação. Elas são muito importantes na hora de gerir, controlar e garantir a qualidade de todos os seus produtos e ser-

viços. Agora, imagine um conjunto de práticas que podem alinhar todos estes recursos, como softwares e sistemas, com os objetivos e as diretrizes de sua empresa?

Pois bem, esta é a Governança de TI. Criada com o objetivo de planejar e elaborar estratégias que possam dar vantagens competitivas às ferramentas de TI implantadas em uma empresa. As práticas da GTI prometem criar serviços absolutamente confiáveis e disponíveis para que você possa alcançar a excelência do seu negócio.

Governança de TI

A Governança de TI é, basicamente, uma "extensão" da Governança Corporativa (conjunto de ações, políticas, regras e processos que regem uma organização específica) direcionada para a gestão das ferramentas, recursos e soluções em TI. Quando implantada, ela deve ser adotada por todos os usuários de softwares e sistemas, incluindo gerentes e gestores, auditores e diretores.

Entre estas ações descritas no conjunto da Governança de TI, estão práticas que garantem a segurança da informação nos processos executados dentro de uma empresa, disponibilidade e total funcionamento das tecnologias da informação e durabilidade de todo o sistema implantado nestas corporações.

Frameworks da GTI

Para implantar a Governança de TI em sua empresa, é importante que você conheça todos os frameworks – em outras palavras, modelos de trabalho – que fornecem as métricas e o que deve ser feito para garantir a eficácia desta prática.

Os principais frameworks da GTI são:

Cobit (Control Objectives for Information and related Technology)

Este é o modelo de trabalho mais utilizado na Governança de TI e está na sua versão 5. Ele apresenta recursos que incluem sumário executivo, controles de objetivos, mapas de auditorias, indicadores de metas e performances e um guia com técnicas de gerenciamento. Suas práticas de gestão são recomendadas por especialistas da área e ele pode ser utilizado para testar e garantir a qualidade dos serviços de TI prestados, utilizando um sistema de métricas próprio.

ITIL (Information Technology Infrastructure Library)

Este é um framework que é voltado para o público e não para o proprietário. O ITIL define o conjunto de práticas para o gerenciamento dos serviços de TI por meio de "bibliotecas" que fazem parte de cada módulo de gestão. Dessa forma, diferentemente do Cobit, este é um modelo mais focado para os serviços de TI em si.

PmBOK (Project Management Body of Knowledge)

Este framework está voltado para o gerenciamento de projetos da área e melhorar o desenvolvimento e a atuação dos profissionais de TI. Todas as definições, conjuntos de ações e processos do PmBOK estão descritos em seu manual, que expõe as habilidades, ferramentas e técnicas necessárias para realizar a gestão de um projeto.

Como a GTI pode ajudar a minha empresa?

Agora que você conhece um pouco mais sobre a Governança de TI, é necessário conhecer um pouco melhor sobre as suas vantagens e como ela pode ajudar a sua empresa. Basicamente, a implantação de suas práticas promove a segurança de toda a informação que circula no interior de seus sistemas e softwares, assim como garante a durabilidade e eficácia de todos os recursos de TI que estão em uma organização. Dessa forma, é possível:

Evitar que dados e informações sigilosas sobre a sua empresa sejam vazados, causando enormes danos aos seus negócios;

Garantir a automatização dos processos e das tarefas específicas, economizando, assim, tempo e dinheiro;

Assegurar a eficácia e facilitar a utilização das ferramentas e recursos de TI dentro de sua empresa, pois com a sua implantação, há menos riscos de bugs, paradas ou fatores que comprometam o seu funcionamento;

Melhorar e inovar os processos de gestão, marketing e vendas de seus negócios, tornando assim a sua empresa mais competitiva;

Antecipar os problemas e os riscos que podem prejudicar os seus negócios e, dessa forma, garantir mais precisão nas suas decisões.

Conhecer melhor todo o funcionamento da Governança de TI e as suas vantagens já é o primeiro passo para a sua implantação, a fim de garantir a melhoria de seus serviços e produtos. Se você se sentiu atraído pela ideia, não hesite em apostar e investir nela. Esta é a melhor forma de conquistar o sucesso do uso de TI em sua empresa.

Os avanços da tecnologia no tratamento da informação colocam a área de TI numa posição de grande importância dentro das organizações. Um investimento em TI não se trata de um investimento em um setor apenas, mas de investir na própria empresa como um todo, afinal, a tecnologia é um agente significativo e transformador no processo de gestão.

Considerando o peso que TI tem nas empresas e as novas formas de organização que ela promove, ter controle sobre os processos da sua empresa torna-se indispensável para garantir o sucesso do negócio. a governança de TI pode ser pensada, portanto, como a gestão da gestão, mas equivale, sobretudo, a um conjunto de práticas que deve orientar o CIO na tomada de decisão para o alcance dos objetivos da empresa. Saiba um pouco mais sobre governança de TI e descubra a importância dela para as empresas.

Entendendo o Conceito de Governança em TI

Ser mais produtiva e tirar o melhor proveito dos recursos tecnológicos nos quais investiu são ambições de qualquer empresa atuante no mercado. No entanto, a realidade mostra que, embora as organizações dependam bastante de TI, os orçamentos tornam-se cada vez mais limitados, e conseguir aprovação de projetos para o setor não é fácil.

Colocar em prática um programa de governança de TI, é implementar ações que primem por um alinhamento do setor com as diretrizes e objetivos da empresa. É desenvolver e aplicar um conjunto de práticas estruturadas que otimizem a atuação do setor para servir aos propósitos da organização.

O programa de governança vai envolver não só aspectos operacionais, mas também impactar nas questões legais, normas ou regulamentações que a empresa deva cumprir para estar em conformidade com a lei.

Falar em governança de TI é falar de padrões e de relacionamentos construídos de forma estruturada. Requer a participação não só dos profissionais técnicos, mas também de diretores, gestores e também dos usuários da tecnologia. A ideia é garantir, com o envolvimento de todos, um controle efetivo dos processos, principalmente no que diz respeito à segurança das informações.

É também objetivo da governança de TI minimizar riscos. Empresas que alcançaram sucesso em seus processos de gestão trabalham sob a perspectiva da minimização dos riscos. É um comportamento baseado em planejamento, suficientemente realista, que corresponde a atuar de forma preventiva, antecipando soluções para eventuais problemas antes que possam impactar no equilíbrio da empresa.

Importância da Governança de TI para a Gestão Estratégica

Alinhar definitivamente as ações de TI à estratégia da empresa significa alcançar mais produtividade e otimização dos recursos destinados ao setor, ou seja, fazer mais com menos. O propósito por trás da implementação da governança em TI é fazer com que a empresa opere seus processos em TI de maneira fluida, com sincronia, a funcionar como se fossem engrenagens. É trazer mais controle para a função de TI na empresa, de maneira que agregue valor ao negócio, criando uma relação mais equilibrada entre riscos e retorno. A aplicação de “estruturas” tem o papel de trazer uma nova ordem aos processos, direcionando-os para contribuir efetivamente com a estratégia da organização.

Adaptação À Realidade De Cada Empresa

O fato de ter gerado bons resultados numa empresa não significa que o mesmo programa de governança possa ser aplicado em outra. Servem apenas de base para orientação. O melhor é que cada programa considere o universo particular da empresa, especificidades, dificuldades, aspectos da cultura e estrutura organizacionais.

Implantação De Melhores Práticas

Quando se fala em implementação de “estruturas”, “conjunto de práticas” ou “melhores práticas”, significa a menção de modelos específicos que servem de guias e podem ser seguidos pelas empresas ao aplicar um programa de governança de TI.

O objetivo dos guias é fornecer conjuntos de práticas que orientem o programa de governança, sempre aliado aos objetivos da empresa.

Implantar melhores práticas significa, muitas vezes, mudar paradigmas e padronizar novos processos. Por isso, a escolha do modelo deve ser feita com cautela e considerar os interesses e necessidades da organização.

Alguns dos mais conhecidos modelos de referência para gestão de TI são:

ITIL (Information Technology Infrastructure Library)

CobIT (Control Objectives for Information and related Technology);

CMMI (Capability Maturity Model Integration), Modelo Integrado de Maturidade e de Capacidade;

NBR ISO 17799

Sendo o CobIT mais voltado para a melhoria do ROI (retorno sobre investimento), trabalhando, para isso, com métricas e avaliação de KPI (Key Performance Indicators), KGI (Key Goal Indicators) e CSF (Critical Success Factors).

Já o ITIL envolve orientações para gerenciar infraestrutura e avaliar o desempenho dos recursos, também utilizando métricas e indicadores para isso.

Framework

São as próprias estruturas dos modelos dos quais falamos antes. Correspondem a um conjunto consolidado das melhores práticas. Em geral, são desenvolvidos por profissionais da área de TI incentivados por grandes empresas ou por estímulos governamentais.

Desafios

Talvez o principal deles, quando se considera a aplicação de um programa de governança de TI, seja descobrir e determinar, com clareza e objetividade, quais requisitos a empresa deve levar em conta. A governança deve estar firmemente alinhada aos objetivos estratégicos do negócio, mas também de acordo com a legislação, inclusive considerando as recomendações dos órgãos de fiscalização do Governo.

Retomar O Potencial De Ti Na Empresa

Consta que deva ser uma preocupação dos administradores, melhor dirigir e controlar os efeitos de TI na estratégia na empresa, a fim de reafirmar o valor do setor para o negócio. É fundamental que a importância da área de TI fique clara, tanto para os profissionais técnicos quanto para os diretores, e só assim as ações terão eficácia.

Fica claro que o processo de tomada de decisão em TI será melhor conduzido se respaldado em definições de governança de TI. Reorganizar os processos no setor, alinhando as estruturas às estratégias da empresa, significa retomar o controle sobre o potencial que a TI representa no sucesso da empresa.

Conseguiu entender melhor o que é governança de TI? Tem dúvidas ou quer compartilhar opiniões? Deixe um comentário e continue acompanhando nossas publicações!

ISO/IEC 38500 - Governança Corporativa de Tecnologia da Informação

A norma ISO/IEC 38500 tem como objetivo fornecer uma estrutura de princípios para os dirigentes utilizarem na avaliação, gerenciamento e no monitoramento do uso da tecnologia da informação nas suas organizações.

Para encontrar a norma basta visitar o site da Associação Brasileira de Normas Técnicas (ABNT) e procurar a norma NBR ISO/IEC 38500:2009.

Podemos aplicar a norma ISO/IEC 38500 em qualquer organização podendo ser pública ou privada e de diferentes tamanhos objetivando promover o uso eficaz, eficiente e aceitável da Tecnologia da Informação nas organizações. Utilizar a norma garante aos consumidores, acionistas, funcionários e demais interessados que se a norma for seguida pode-se confiar na governança corporativa de TI na organização, além de informar e orientar os dirigentes quanto ao uso da TI na organização e fornecer uma base para uma avaliação da governança corporativa de TI**.**

Esta norma não é objeto de certificação, mas traz conceitos muito importantes sobre governança de TI e que podem ser úteis no entendimento, pela alta direção, de suas responsabilidades em relação a TI.

Portanto, podemos verificar que esta norma avalia e direciona o uso da TI para oferecer suporte à organização e monitorar seu uso para realizar os planos.

Estrutura

A norma afirma que existem seis princípios que caracterizam uma boa governança de TI, são eles:

Responsabilidade: este princípio diz que os indivíduos e os grupos dentro da organização compreendem e aceitam as suas responsabilidades.

Estratégia: este princípio diz que a estratégia de negócio da organização deve levar em consideração as capacidades atuais e futuras da TI.

Aquisição: este princípio diz que as aquisições da TI são realizadas por razões válidas, com base em análise apropriada e de forma contínua, com decisões claras e transparentes equilibrando os benefícios, oportunidades, custos e riscos, de curto e longo prazo.

Desempenho: este princípio diz que a TI deve apoiar a organização oferecendo serviços, níveis de serviço e qualidade de serviço que sejam necessários para atender aos requisitos atuais e futuros de negócio.

Conformidade: este princípio diz que a TI cumpre a legislação e os regulamentos obrigatórios. Todas as políticas e as práticas são claramente definidas, implantadas e fiscalizadas.

Comportamento Humano: este princípio diz que todas as políticas, práticas e decisões da TI demonstram respeito pelo comportamento humano, incluindo as necessidades atuais e futuras das pessoas envolvidas no processo.

Além de definir os princípios a norma também preconiza que os dirigentes governem a TI através de três tarefas principais:

Avaliar o uso atual e futuro da TI incluindo estratégias, propostas e os fornecedores.

Orientar a preparação e a implementação de planos e políticas para assegurar que o uso da TI atenda aos objetivos do negócio.

Monitorar que as políticas e o desempenho definido nos planos estejam sendo seguidos.

Segundo a norma devemos aplicar o ciclo Avaliar-Dirigir-Monitorar em cada um dos princípios definidos anteriormente. Dessa forma teríamos:

Responsabilidade: Aplicando a tarefa Avaliar do ciclo temos que no principio da Responsabilidade devemos avaliar as reponsabilidades. Aplicando a tarefa de Dirigir temos que neste princípio devemos exigir que os planos fossem cumpridos de acordo com as responsabilidades que foram delegadas. E por fim, na tarefa de Monitorar temos que neste princípio devemos monitorar que os mecanismos apropriados de governança de TI sejam estabelecidos, garantir que aqueles que receberam responsabilidades reconheçam e compreendam suas responsabilidades e monitorar o desempenho daqueles a que foram dadas as responsabilidades quanto a governança de TI.

Estratégia: Aplicando a tarefa Avaliar tem-se que no princípio da Estratégia devemos avaliar se os desenvolvimentos da TI estão apoiando o negócio, se a TI está alinhada com os negócios de acordo com seus planos e políticas, e o risco atual da TI para o negócio. Aplicando a tarefa de Dirigir temos que neste princípio devemos preparar planos e políticas para que a organização seja beneficiada com o uso da TI, encorajando o dirigente a apresentar propostas inovadoras para a TI. E por fim, na tarefa de Monitorar temos que neste princípio devemos monitorar o progresso das propostas de TI aprovadas verificando se os benefícios com a TI estão sendo alcançados.

Aquisição: Aplicando a tarefa Avaliar tem-se que no princípio da Aquisição devemos avaliar as opções de fornecimento da TI. Aplicando a tarefa de Dirigir temos que neste princípio devemos orientar para que os ativos de TI sejam adquiridos de forma apropriada e devemos certificar-se de que os acordos de fornecimento darão suporte necessário às necessidades da organização. E por fim, na tarefa de Monitorar temos que neste princípio devemos monitorar os investimentos de TI e garantir a compreensão mútua dos objetivos da aquisição por parte da organização e dos fornecedores.

Desempenho: Aplicando a tarefa Avaliar tem-se que no principio do Desempenho devemos avaliar as ideias ou propostas dos gerentes, avaliar os riscos relacionados à continuidade do negócio, riscos quanto à integridade da informação e à proteção dos ativos de TI e avaliar a eficácia e o desempenho do sistema de governança. Aplicando a tarefa de Dirigir temos que neste princípio devemos garantir a alocação de recursos suficientes para que a TI atenda às necessidades da organização dadas às prioridades acordadas e as restrições de orçamento. E por fim, na tarefa de Monitorar temos que neste princípio devemos monitorar até onde a TI dá suporte ao negócio, se os recursos foram priorizados de acordo com os objetivos e se as políticas estão sendo seguidas corretamente.

Conformidade: Aplicando a tarefa Avaliar tem-se que no principio da Conformidade devemos avaliar até onde a TI cumpre com as obrigações de conformidade interna e externa. Aplicando a tarefa de Dirigir temos que neste princípio devemos garantir que a TI esteja de acordo com as exigências legais, que as políticas estejam estabelecidas e sendo cumpridas e que as ações de TI sejam sempre éticas. E por fim, na tarefa de Monitorar temos que neste princípio devemos monitorar o cumprimento e conformidade da TI por meio de auditorias, monitorar as atividades de TI para garantir o cumprimento das exigências de privacidade, gerenciamento, conhecimentos estratégico, preservação da memória organizacional e ambiental.

Comportamento Humano: Aplicando a tarefa Avaliar tem-se que no principio do Comportamento Humano devemos avaliar as atividades de TI para garantir que os comportamentos humanos sejam identificados e considerados. Aplicando a tarefa de Dirigir temos que neste princípio devemos exigir que as atividades de TI sejam compatíveis com as diferenças de comportamento humano, que os riscos, oportunidades, constatações e preocupações sejam identificados e relatados por qualquer pessoa a qualquer momento. E por fim, na tarefa de Monitorar temos que neste princípio devemos monitorar as atividades de TI para garantir que os comportamentos humanos identificados permaneçam relevantes e que lhe sejam dadas a devida atenção.

Usando esta norma temos como benefício uma melhor avaliação dos riscos da TI para o negócio e um melhor aproveitamento das oportunidades com o uso da TI na organização. Além disso, temos como benefício a garantia do cumprimento das obrigações regulamentares, legislativas, legais, contratuais, e por fim, que o uso da TI contribua de forma positiva para o bom desempenho da organização através da correta implementação e operação dos ativos de TI, maior clareza quantos as responsabilidades, continuidade e sustentabilidade do negócio, alinhamento entre TI e o negócio e inovação dos serviços necessários ao negócio, redução de custos.

COBIT – Control Objectives for Information and related Technology

O CobiT (Control Objectives for Information and related Technology) foi criado em 1994 pela ISACF23 e desde lá vem evoluindo com a incorporação de padrões internacionais técnicos, profissionais, regulatórios e específicos para processos de TI. A segunda e terceira edição do Cobit em 1997 e 2000 respectivamente introduziram diversas novidades sendo que a última atualização foi publicada pelo IT Governance Institute (ITGI), órgão criado pela ISACA com o objetivo de promover um melhor entendimento e a adoção dos princípios de Governança de TI. Em 2005 foi publicada a versão 4.0 e em 2007 houve uma atualização incremental (versão 4.1). Ultimamente foi lançada a versão 5.

O principal objetivo do Cobit é contribuir para o sucesso da entrega de produtos e serviços de TI com base nas necessidades do negócio. Dessa forma, o Cobit estabelece relacionamentos com os requisitos do negócio, organiza as atividades de TI em um modelo de processos genéricos, identifica os principais recursos de TI que devem possuir mais investimentos e define os objetivos de controle que devem ser considerados para a gestão.

O Cobit é um modelo genérico que representa todos os processos normalmente encontrados nas funções da TI sendo compreensível tanto para a operação quanto para os gerentes. Além disso, o Cobit é representado por cinco áreas que sustentam o seu núcleo: o alinhamento estratégico que é a ligação entre o negócio e a TI, agregação de valor que se restringe em executar aquilo que entregue benefícios de acordo com a estratégia, gerenciamento de recursos em que se procura otimizar os investimentos, gerenciamento de riscos em que a alta direção conhece e entende os riscos, e a medição de desempenhoem que acompanha-se e monitora-se a implantação e o andamento dos projetos e recursos associados.

Estrutura

O Cobit é o modelo de gestão de TI perfeito quando desejamos integrar e institucionalizar boas práticas de planejamento e organização, aquisição e implementação, entrega e suporte, e monitoramento e avaliação de desempenho da TI. Com isso empresa pode gerenciar de forma eficiente seus investimentos em recursos tecnológicos e suas informações, maximizando assim seus benefícios, oportunidades de negócio e vantagem competitiva no mercado.

Um dos focos do Cobit é no negócio onde o modelo preconiza que para fornecer a informação necessária que a empresa necessita para atingir suas metas de negócio é necessário associá-los às suas metas de TI, utilizando um conjunto estruturado de processos garantindo a entrega dos serviços de TI. Outro foco do Cobit é na orientação para processos onde o Cobit identificou 34 processos de TI e os distribuiu entre quatro domínios que espelham os agrupamentos usuais existentes em uma organização de TI.

Os quatro domínios identificados no Cobit são: Planejamento e Organização (PO) onde atua-se na parte estratégica e tática procurando identificar formas em que a TI pode contribuir para atender aos objetivos do negócio; Aquisição e Implementação (AI) onde identificamos, desenvolvemos e adquirimos soluções de TI para implementar, integrar e executar a estratégia estabelecida; Entrega e Suporte (DS) que é onde entregamos os serviços requeridos, incluindo gerenciamento de segurança e continuidade, suporte aos serviços para os usuários, gestão dos dados e da infraestrutura operacional; Monitoração e Avaliação(ME) é onde assegura-se a qualidade dos processos de TI, assim como a governança e a conformidade com os objetivos de controle, através de acompanhamento, monitoração de controles internos e de avaliações internas e externas.

Mais um foco importante do Cobit é o Controle através de objetivos. O Cobit define como controle o conjunto de políticas, procedimentos, práticas e estruturas organizacionais desenvolvidas para dar uma garantia razoável de que os objetivos de negócio serão atingidos e de que os eventos indesejáveis serão prevenidos ou detectados e corrigidos. Já um objetivo de controle define um resultado desejados ou propósito a ser atingido através da implementação de procedimentos de controle em uma atividade de TI específica. Esses objetivos de controle constituem os requisitos mínimos para que os processos de TI possam ser controlados de forma eficaz.

Dessa forma, as informações de controle extraídas da operação de cada processo de TI são comparadas aos objetivos de controle e com isso as ações corretivas/preventivas necessárias são empreendidas para a melhoria do processo. Alguns controles são genéricos e aplicáveis a todos os processos, entretanto, outros são mais específicos. Outro foco do Cobit é o direcionamento para medições

em que se procura definir o que deve ser medido, como e onde obter os dados e em que perspectiva os resultados devem ser agregados. As empresas precisam medir a situação atual e monitorar as ações de melhoria que foram realizadas em cima disso.

Outra situação importante é analisar a relação custo-benefício do controle. O Cobit ainda propõe um modelo de maturidades baseado em cinco níveis onde cada nível indica a situação atual da organização, permite comparar com a situação das melhores organizações no segmento, comparar com padrões internacionais, estabelecer e monitorar passo a passo as melhorias dos processos, entre outros. A visão integrada do modelo é outro foco importante do Cobit onde o Cobit pode ser definido em função do princípio básico que recursos de TI são gerenciados por processos de TI para atingir metas de TI, que, por sua vez estão estreitamente ligadas aos requisitos do negócio. Por fim, outro foco de modelo é o conteúdo dos processos de TI em que os processos de TI estão organizados na documentação do modelo de forma a mostrar uma visão completa como devem ser controlados, gerenciados e medidos.

O Cobit também possui produtos complementares, além do documento principal, como o "Board Briefing on IT Governance" que é um guia executivo que aborda o entendimento da importância da Governança de TI e das suas principais características, assim como das responsabilidades da alta direção na sua condução, o "Building the Business Case for CobiT and Val IT – Executive Briefing" que mostra uma visão geral de casos de implantação do Cobit e do Val IT em empresas de diversos segmentos, o "Information Security Governance: Guidance for Boards of Directors and Executive Management" que apresenta a segurança da informação nos termos do negócio, entre outros.

Portanto, o Cobit cobre todo o conjunto de atividades de TI, concentrando-se mais em "o que" deve ser atingido em vez de "como" atingir. Assim, o Cobit é recomendado ser utilizado no nível estratégico aplicando-se a toda a organização favorecendo muito o entendimento dos processos de TI e fornecendo um excelente guia para a sua implementação ou melhoria nas organizações, assim como para a avaliação da maturidade atual dos processos existentes.

Val IT

O modelo Val IT foi criado pelo IT Governance Institute (ITGI) devido à necessidade de demonstração de retorno que a TI deve fornecer para o negócio como uma forma de mostrar aos executivos o retorno dos investimentos da TI para o negócio. O modelo foi criado com a ajuda de representantes de empresas e do meio acadêmico, considerando tanto as metodologias existentes como emergentes e o desenvolvimento de pesquisas. O Val IT foi publicado em 2006 e obteve sua versão 2.0 em 2008.

Entre os objetivos do modelo temos o auxilio à gerência para assegurar que as organizações obtenham o máximo de retorno dos investimentos em TI para oferecer suporte ao negócio a um custo razoável e com nível de risco conhecido e aceitável, e outro objetivo é o fornecimento de diretrizes, processos e práticaspara subsidiar a diretoria e a gestão executiva no entendimento e no desempenho dos seus respectivos papéis em relação aos investimentos em TI.

Pode-se dizer que o Val IT é um modelo que estende e complementa o Cobit, visto que este aborda a tomada de decisões em relação aos investimentos em TI e a realização efetiva dos benefícios, enquanto que o Cobit tem um foco maior na execução.

Estrutura

O Val IT tem alguns princípios como: os investimentos em TI devem ser gerenciados como um portfólio de investimentos, os investimentos de TI incluirão o conjunto completo de atividades que são requeridos para atingir o valor para o negócio, os investimentos em TI serão gerenciados através do seu ciclo de vida econômico, as práticas de entrega de valor reconhecerão que há diferentes tipos de investimentos que devem ser avaliados e gerenciados de formas diferentes, as práticas de entrega de valor definirão e monitorarão métricas chaves e responderão rapidamente a mudanças e desvios, práticas de entrega de valor envolverão todos interessados relevantes e atribuirão responsabilidades pelo resultado de forma apropriada para a entrega das capacidades e a realização dos benefícios para o negócio, e as práticas de entrega de valor serão continuamente monitoradas, avaliadas e melhoradas.

O modelo está organizado entre processos e domínios, são eles:

Governança do Valor (VG): este domínio estabelece o framework de governança, incluindo a definição de portfólio para gerenciar os investimentos e os serviços de TI resultante, ativos e recursos.

Os processos do domínio são: "VG1 – Estabelecer uma liderança informada e comprometida" onde é estabelecida uma liderança informada e comprometida em um fórum de liderança e uma subordinação do CIO conforme a importância da TI para a organização, também é desenvolvido um entendimento adequado dos elementos chaves da governança e abordagens claras na estratégia da empresa para a TI e assegura o alinhamento e a integração do negócio com a TI; O processo "VG2 – Definir e implementar processos" define um framework de governança para gestão do valor de TI, avalia a qualidade e cobertura dos processos atuais, define os requisitos dos futuros processos, se estabelecem as estruturas organizacionais e implementa-se os processos considerando os papéis e as responsabilidades correspondentes. O processo "VG3 – Definir as características do portfólio" define os diferentes tipos de portfólio, as categorias em cada portfólio, se desenvolve e comunica-se como essas categorias serão avaliadas comparativamente e de forma transparente e define-se os requisitos para os pontos de revisão para cada categoria. O processo "VG4 – Alinhar e integrar a gestão do valor ao planejamento financeiro da organização" reavalia as práticas atuais de elaboração do orçamento da organização, identifica e implementa as mudanças necessárias. O processo "VG5 – Estabelecer o monitoramento efetivo da governança" é onde se identifica as métricas e metas de resultado para o gerenciamento dos processos de gestão do valor a serem monitorados, identifica abordagens, métodos, técnicas e processos para capturar e comunicar as informações sobre essas medições e também estabelece como os desvios ou problemas serão identificados, monitorados e comunicados. O processo "VG6 – Aperfeiçoar continuamente as práticas de gestão do valor" é onde se analisa as lições aprendidas da gestão do valor, planeja-se, inicia e monitora as mudanças para o aperfeiçoamento da gestão do valor e os processos de gerenciamento do portfólio e do investimento.

Gerenciamento do Portfólio (PM): estabelece qual será o direcionamento estratégico para os investimentos, as características do portfólio de investimento e as restrições de recursos e fundos a partir das quais as decisões sobre o portfólio têm que ser feitas.

Os processos do domínio são: "PM1 – Estabelecer a direção estratégica e um mix de investimentos alvos" onde se procura rever e assegurar a estratégia do negócio, identificar e comunicar oportunidades para TI apoiar a estratégia, definir um mix de investimentos baseado em taxa de retorno, ao grau de risco e tipos de benefícios para os programas no portfólio que implementam a estratégia, ajudar a estratégia do negócio quando necessário e traduzi-la para a estratégia e os objetivos de TI. O processo "PM2 – Determinar a disponibilidade e fontes de fundos" é onde se determina as fontes potenciais de financiamento para os programas, os níveis de financiamento que podem ser obtidos e os métodos necessários para obtê-los, e determinar as implicações da fonte de financiamento sobre as expectativas de retorno. O processo "PM3 – Gerenciar a disponibilidade de recursos humanos" é onde se cria e mantem-se os recursos do negócio e da TI, entende-se a demanda atual e futura por recursos humanos, identifica-se restrições e escassez, cria-se e mantem-se planos táticos para o gerenciamento de RH, monitora-se e reveem-se os planos e as estruturas organizacionais e ajuda-o quando necessário. O processo "PM4 – Avaliar e selecionar programas para receber fundos" é onde se avalia os casos de negócio dos programas, atribui-se um score, toma-se decisões e os comunicamos com base na visão geral do portfólio de investimentos e nos scores individuais de cada programa, alocam-se fundos, revisam-se os programas em seus pontos de controle, movem-se os programas selecionados para o portfólio de investimentos ativos ajustando as metas, previsões e orçamento do negócio. O processo "PM5 – Monitorar e comunicar o desempenho do portfólio de investimento" é onde se procura fornecer uma visão abrangente e exata do desempenho do portfólio de investimento de forma a permitir revisões do progresso em relação às metas do negócio por parte dos stakeholders. O processo "PM6 – Otimizar o desempenho do portfólio de investimento" é onde procura-se rever periodicamente o desempenho do portfólio de investimento e otimizar para novas oportunidades e mudanças de riscos.

Gerenciamento do Investimento (IM): define os programas potenciais baseado em requisitos do negócio, determina se devem ser considerados para análise posterior e desenvolve os casos de negócio para os programas de investimentos candidatos para avaliação pelo gerenciamento do portfólio.

Os processos do domínio são: "IM1 – Desenvolver e avaliar o Business Case inicial do programa" onde se procura reconhecer oportunidades de investimento, classificar as oportunidades com as categorias do portfólio, clarificar os resultados esperados para o negócio e fornecer uma visão de alto nível para todas as iniciativas requeridas para atingir os resultados e como podem ser medidos, for-

necer uma estimativa inicial de benefícios e custos, e determinar se a oportunidade merece um caso de negócio detalhado. O processo "IM2 – Entender o programa candidato e opções de implementação" é onde envolvemos todos os stakeholders chaves para desenvolver e documentar o entendimento completo dos resultados esperados para o negócio a partir do programa candidato, considerando como os resultados serão medidos, o escopo de cada iniciativa para atingir os resultados, os riscos envolvidos e o impacto em todos os aspectos da organização, identificar e avaliar cursos de ação alternativos para obter os resultados para o negócio. O processo "IM3 – Desenvolver o plano do programa" é onde se procura definir e documentar todos os projetos requeridos para atingir os resultados do programa para o negócio, especificar os requisitos de recursos do programa para o negócio e fornecer um cronograma que leve em consideração as interdependências entre os diversos programas.

O processo "IM4 – Desenvolver os custos e benefícios do ciclo de vida" é onde preparamos um orçamento para o programa, listamos os benefícios para o negócio, identificamos e documentamos as metas de resultados esperadas, e submetemos orçamentos, custos, benefícios e planos associados para revisão, refinamento e aprovação. O processo "IM5 – Desenvolver, em detalhe, o Business Case do programa candidato" é onde se procura desenvolver um caso de negócio abrangente e completo do programa contemplando propósito, objetivos, abordagens e escopo, dependências, riscos, pontos de controle e impactos de mudanças organizacionais. Inclui avaliação do valor, taxa de retorno, alinhamento estratégico e principais premissas, fornece um plano do programa cobrindo os projetos componentes, plano de realização de benefícios, gerenciamento da mudança e a estrutura para o gerenciamento do programa, atribui responsabilidades pelo atendimento aos benefícios, controle de custos, riscos e obtêm concordância e aceitação das responsabilidades.

O processo "IM6 – Lançar e gerenciar o programa" é onde procura-se planejar, alocar recursos e comissionar os projetos necessários para atender aos resultados do programa. Também planejamos recursos, orçamento, gerenciamos o desempenho do programa contra critérios chaves, identificamos desvios do plano e tomamos ações de remediação, monitoramos o desempenho de cada projeto contra seus critérios, monitoramos os benefícios durante o desenvolvimento do programa, verificamos os benefícios obtidos, avaliamos probabilidades de atendimentos abaixo ou acima dos resultados e comunicamos o progresso dos benefícios e iniciarmos ações corretivas a tempo para os desvios significantes do plano. O processo "IM7 – Atualizar os portfólios operacionais de TI" é onde refletimos as mudanças resultantes no programa de investimento sobre os serviços relevantes de TI, ativos e recursos. O processo "IM8 – Atualizar o Business Case" é onde atualizamos o caso de negócio do programa para refletir o status atual sempre que ocorrer qualquer mudança em custos e benefícios projetados, riscos e oportunidades.

O processo "IM9 – Monitorar e comunicar sobre o programa" é onde monitoramos o desempenho de todo o programa e de todos os projetos e comunicamos para os Comitês Executivos apropriados. A comunicação inclui o desempenho do plano do programa (cronograma e orçamento), completude e qualidade de funcionalidades entregues, o status de controles internos e da mitigação de riscos e a manutenção da aceitação pelas responsabilidades. O processo "IM10 – Encerrar o programa" é onde procura-se encerrar o programa e removê-lo do portfólio de investimento quando houver concordância das partes interessadas de que os benefícios foram alcançados ou que não serão alcançados com os critérios de avaliação do programa.

Portanto, o Val IT demonstra claramente o planejamento e a gestão dos investimentos em TI, a gestão de programas de investimento em TI, a gestão do portfólio de TI e a implementação de um processo para o planejamento e a gestão de investimentos e do portfólio de TI. O objetivo claro do Val IT é demonstrar o valor que a TI gera para o negócio, porém implementar os seus processos demanda uma mudança cultural muito intensa, além de métodos, técnicas analíticas sobre itens de informação relevantes tanto para o negócio quanto para a operação de TI e que envolvem uma cadeia organizacional de responsabilidades relativamente complexa.

Os benefícios mais evidentes com a utilização do Val IT é o aumento de entendimento e transparência dos custos, riscos e benefícios dos investimentos de TI, aumento da probabilidade da seleção dos melhores investimentos, aumento da possibilidade de sucesso dos investimentos, maior controle sobre a realização dos benefícios dos investimentos, investimentos alinhados com a estratégia da empresa, possibilidade de alinhar rapidamente os investimentos face às mudanças no negócio, maior facilidade de comunicação entre TI e negócio e o CIO consegue mais claramente demonstrar o valor dos investimentos em TI.

O Framework Risk IT

O Risk IT foi desenvolvido pela ISACA com a participação de vários especialistas e foi incialmente publicado em 2009. O modelo é utilizado para auxiliar no gerenciamento de riscos relacionados a TI. Assim como o Val IT o Risk IT também é um complemento do Cobit.

Entre os objetivos do modelo estão: integrar o gerenciamento de risco de TI com o Sistema de Gerenciamento de Riscos da Organização, tomar decisões bem informadas sobre a extensão dos riscos, saber qual a tolerância e o apetite por riscos da organização e entender como responder aos riscos.

Estrutura

Os princípios fundamentais do Risk IT são: conectar os riscos de TI aos objetivos do negócio, garantir que todo risco de TI é um risco de negócio, focar no resultado do negócio com a TI apoiando o atingimentos dos objetivos do negócio e expressando os riscos em termos de impacto sobre o atendimento dos objetivos ou da estratégia do negócio, desenvolver a análise de riscos que contemple uma análise de dependência do processo de negócio em relação a recursos de TI, apoiar o gerenciamento de riscos de TI como um habilitador do negócio e não um inibidor. Além disso, a governança dos ricos de TI deve estar alinhada ao Sistema de Gerenciamento de Riscos da organização e a quantidade de risco que a empresa está disposta a lidar deve estar claramente definida.

O modelo afirma que Risco de TI é o risco do negócio associado com uso, propriedades, operação, envolvimento, influência e adoção da TI dentro da empresa e consiste de eventos e condições relacionados com a TI que podem ter potencial para impactar o negócio.

Basicamente o Risk IT é estruturado em atividades chaves, processos e domínios, e assim como o CobiT, o Risk IT Framework também é composto por um Guia Gerencial, um quadro RACI (Responsible, Accountable, Consulted and Informed) e um esquema de métricas e entradas e saídas dos processos e modelo de maturidade.

Detalhando os domínios e processos do Risk IT temos que o domínio de Governança do Risco é composto por três processos e dezesseis atividades, são eles:

Estabelecer e manter uma visão comum dos riscos: este processo assegura que as atividades de gerenciamento de riscos estejam alinhadas com a capacidade da organização de lidar com perdas relacionadas à TI e com a tolerância subjetiva das lideranças ao risco. Este processo tem as seguintes atividades: Realizar a avaliação dos riscos da organização, Propor limites para a tolerância aos riscos de TI, Aprovar a tolerância aos riscos de TI, Alinhar a política de riscos de TI, Ppromover uma cultura de conscientização para os riscos de TI, Encorajar uma comunicação efetiva sobre os riscos de TI.

Integrar com o Sistema de Gerenciamento de Riscos da Organização: este processo integrar a estratégia e as operações de riscos de TI com as decisões estratégicas sobre riscos que são tomadas no âmbito da organização. Este processo tem como atividades: Estabelecer e manter as responsabilidades pelo gerenciamento dos riscos de TI, Coordenar as estratégias de risco de TI e da organização, Adaptar as práticas de risco de TI às práticas de riscos da organização, Prover recursos adequados para o gerenciamento de riscos, Auditar de forma independente o gerenciamento dos riscos de TI.

Tomar decisões de negócios conscientes dos riscos: este processo assegura que as decisões da organização considerem todas as oportunidades e consequências da dependência do sucesso da TI. Este processo tem as seguintes atividades: Obter o apoio da administração para a abordagem de análise dos riscos de TI, Aprovar a análise dos riscos de TI, Embutir considerações de riscos de TI na tomada das decisões estratégicas de negócio, Aceitar os riscos de TI, Priorizar as atividades de resposta ao risco.

O domínio de Avaliação do Risco é composto por três processos e quatorze atividades, são eles:

Coletar dados: este processo procura obter dados relevantes para identificação, análise e comunicação dos riscos. Este processo tem as seguintes atividades: Estabelecer e manter um modelo para a coleta de dados, Coletar dados no ambiente operacional, Coletar dados sobre eventos de risco, Identificar fatores de risco.

Analisar o risco: coletar informações úteis para apoiar as decisões relativas a riscos que levem em consideração os fatores de riscos relevantes para o negócio. Este processo tem as seguintes atividades: Definir o escopo da análise do risco, Estimar o risco de TI, Identificar opções de resposta ao risco, Realizar um peer review na análise dos riscos de TI.

Manter o perfil do risco: manter um inventário completo e atualizado de todos os riscos e atributos conhecidos, recursos de TI, capacidades e controles, no contexto dos produtos, processos e serviços do negócio. Este processo tem as seguintes atividades: Mapear os recursos de TI que apoiam os processos de negócio, Determinar a criticidade dos recursos de TI para o negócio, Entender as capacidades da TI, Atualizar os componentes dos cenários de riscos de TI, Manter os registros e o mapa de riscos de TI, Desenvolver indicadores de riscos de TI.

O domínio de Resposta ao Risco é composto por três processos e treze atividades, são eles:

Articular os riscos: assegurar que as informações sobre a realidade das exposições ao risco e as oportunidades estejam disponíveis, no tempo adequado, para as pessoas corretas, para que haja uma resposta apropriada. Este processo tem as seguintes atividades: Comunicar os resultados da análise dos riscos, Comunicar as atividades de gerenciamento dos riscos e a situação de conformidade, Interpretar os resultados das auditorias independentes de TI, Identificar as oportunidades relacionadas à TI.

Gerenciar os riscos: assegurar que as iniciativas para aproveitar oportunidades e reduzir os riscos sejam gerenciadas como um portfólio.

Este processo tem as seguintes atividades: Inventariar os controles, Monitorar o alinhamento operacional com os limites de tolerância aos riscos, Responder às exposições a riscos e oportunidades identificadas, Implementar controles, Comunicar o progresso do plano de ação para os riscos.

Reagir aos eventos: assegurar que as iniciativas para aproveitar oportunidades ou para limitar as perdas com os eventos relacionados à TI sejam ativadas em tempo hábil e sejam efetivas. Este processo tem as seguintes atividades: Manter planos de respostas a incidentes, Monitorar o risco de TI, Iniciar respostas aos incidentes, Comunicar lições aprendidas a partir dos eventos de risco.

Portanto, o Risk IT reduz as perdas para a organização em função de um evento de risco que tenha impacto, reduz as perdas em função do não investimento em novas oportunidades com o apoio da TI, provê um guia bastante abrangente para o gerenciamento dos riscos relacionados à TI, integra o gerenciamento de risco da TI com o da organização e fornece uma linguagem comum acerca de riscos para toda organização.