

CobIT 4.01 – OBJETIVOS DE CONTROLE PARA INFORMAÇÃO E TECNOLOGIAS RELACIONADAS

**METODOLOGIA DE AUDITORIA
PARA AVALIAÇÃO DE CONTROLES
E CUMPRIMENTO DE PROCESSOS
DE TI**

**NARDON, NASI
AUDITORES E CONSULTORES**

CobiT 4.01 - MISSÃO

- A missão do **CobiT** foi definida pelo IT Governance Institute como:
- Pesquisar, desenvolver, publicar e promover um conjunto atualizado, autorizado e com foco internacional, de objetivos de controle geralmente aceitos e aplicáveis à tecnologia da informação para serem usados por gestores de TI, usuários e auditores de sistemas.

CobiT 4.01 – CONCEITOS

- O **CobiT** é uma referência mundial utilizada na avaliação de controles e cumprimento dos processos de TI, sendo amplamente adotado pelas empresas em todo o mundo
- O **CobiT** é um conjunto de diretrizes baseadas em auditoria de processos, práticas e controles de TI

CobiT 4.01 - CONCEITOS

- O **CobiT** não determina como os processos de TI devem ser estruturados, porém orienta sobre os controles que eles devem ter para que a TI cumpra seus objetivos em termos de governança

CobiT 4.01 - CONCEITOS

- Quatro fatores são essenciais para atingir os objetivos:
- A) alinhamento e entrega de valor pela área de TI para os negócios
- B) correta alocação e medição dos recursos envolvidos
- C) avaliação para redução dos riscos de TI
- D) atendimento de padrões regulatórios

ORIGEM DO **CobiT**

- O **CobiT** foi desenvolvido a partir do Committee of Sponsoring Organizations of the Treadway Commission – internal control – Integrated Framework (COSO)
- É um trabalho conjunto da Information Systems Audit and Control Foundation, da IT Governance e patrocinadores do **CobiT**, reunindo especialistas de vários países, coordenados pelo Comitê Executivo do **CobiT**

EVOLUÇÃO DO **CobiT**

- 1996 – primeira versão do **CobiT** lançada pelo ISACA (Information Systems Audit and Control)
- 1998 – segunda versão: lança um conjunto de objetivos de controle para aplicações de negócios
- 2000 – terceira versão: inclui normas e guias associadas a gestão

EVOLUÇÃO DO **CobIT**

- 2002 – Sarbanes Oxley Act – impacto significativo na adoção do **CobIT** nos EUA e nas empresas globais que atuam nos EUA
- 2005 – Quarta versão: melhoria dos controles voltada a segurança e disponibilidades de TI na organização

COBIT 4.01 E O AMBIENTE DAS EMPRESAS

- A informação é um dos ativos mais valiosos para uma organização.
- Organizações de sucesso reconhecem os benefícios da tecnologia da informação (TI) e os utilizam para agregar valor ao negócio, com vantagens à todos os interessados em seu desempenho (stakeholders)

CobiT 4.01 E O AMBIENTE DAS EMPRESAS

- Há uma crescente dependência da informação
- Esta dependência está atrelada aos sistemas que geram as informações
- A vulnerabilidade dos sistemas e das informações é uma ameaça, interna e externa, às organizações

COBIT 4.01 E O AMBIENTE DAS EMPRESAS

- Há uma escala de necessidades e custo dos investimentos, atuais e futuros, para a obtenção a informação e no uso da tecnologia da informação
- Há um influência cada vez maior da tecnologia nas empresas e em seus negócios
- O bom uso da TI cria novas oportunidades de negócios, ajuda a racionalizar tarefas e a reduzir custos

CobiT 4.01 E O AMBIENTE DAS EMPRESAS

- Se informação e tecnologia são ativos valiosos, num mundo competitivo e globalizado, a tecnologia da informação bem implementada, voltada ao negócio, pode ser o diferencial
- Para tanto, a TI de uma organização deve estar apoiada no tripé: qualidade, funcionalidade e facilidade de uso

APLICAÇÃO DO CobiT

- O **CobiT** foi projetado para utilização por três distintos públicos:
- **Administradores:** como instrumento de avaliação entre risco e investimento e controle do ambiente de TI
- **Usuários:** certificação de segurança dos serviços fornecidos por TI (internos ou externos)
- **Audidores de Sistemas:** permitir uma avaliação padronizada para fundamentar a sua opinião sobre o TI da organização e permitir apresentar recomendações à administração sobre melhoria dos controles internos

ESTRUTURA DO CobiT 4.01

- O **CobiT** está estruturado através de um Marco Referencial que tem um conjunto de 34 objetivos de controle, um para cada processo de TI, e agrupados em 4 domínios:
 - 1) planejamento e organização;
 - 2) aquisição e implementação;
 - 3) entrega dos serviços;
 - 4) suporte e monitoramento (supervisão).
- Os 34 objetivos estão alicerçados em 318 procedimentos de controle

TI E GOVERNANÇA DE TI

- A tecnologia da informação deve estar voltada aos processos do negócio
- A falta de integração e comunicação entre a Governança de TI e a Governança Corporativa é uma das causas determinantes do fracasso da TI nas organizações

TI E GOVERNANÇA DE TI

- A Governança de TI deve estar voltada para a administração e controle de:
 - 1) Processos de TI da organização;
 - 2) Recursos (materiais e humanos) de TI aplicados pela organização;
 - 3) Geração da informação
- Tudo deve estar direcionado ao negócio da organização e seus objetivos estratégicos

TI E A GOVERNANÇA DE TI

- A Governança de TI conduz a empresa para um processo de informação permanente e coordenado, visando:
 - A) maximizar os benefícios que a TI propicia à organização;
 - B) capitalizar oportunidades;
 - C) obter vantagens competitivas.

O CobiT E A GOVERNANÇA CORPORATIVA

- O **CobiT** ajuda a administração a construir uma ponte entre os riscos do negócio, os controles necessários ao negócio e os aspectos tecnológicos.
- O **CobiT** também ajuda na implantação das melhores práticas de TI, na otimização dos investimentos em TI e estabelece mecanismos de medição, especialmente quando a implantação de sistemas der errado.

O CobiT E A GOVERNANÇA CORPORATIVA

- O controle interno é de responsabilidade da administração
- Os controles internos devem ser adequados ao porte, complexidade e tipo de negócio, funcionando de forma coordenada, integrada e permanente

O Cobit E A GOVERNANÇA CORPORATIVA

- Um sistema de controle interno está alicerçado em quatro pilares:
- A) políticas de controle interno;
- B) estrutura do sistema de controle interno;
- C) práticas para controle das transações;
- D) procedimentos de controle interno.

O **CobiT** E A GOVERNANÇA CORPORATIVA

- O foco principal do **CobiT** é a orientação ao negócio
- Quanto maior é o negócio mais delegação de poderes é necessária;
- Deve haver uma maior capacitação para os donos dos processos, diretores e gerentes, para que estes assumam responsabilidades sobre os processos do negócio

O CobiT E A GOVERNANÇA CORPORATIVA

- O **CobiT** estabelece sete categorias de informação para a Governança Corporativa:
- 1) **Eficácia** – que a informação relevante seja pertinente para o processo do negócio e sua entrega seja oportuna, correta e consistente para a utilização dos interessados;

O CobiT E A GOVERNANÇA CORPORATIVA

- **Eficiência:** prover a informação através da utilização mais produtiva e econômica dos recursos disponíveis;
- **Confidencialidade:** proteção da informação confidencial contra divulgação não autorizada;
- **Integridade:** precisão, suficiência e validade da informação, de acordo com os valores e expectativas do negócio;
- **Disponibilidade:** tornar a informação disponível quando esta é requerida pelo processo do negócio

O CobiT E A GOVERNANÇA CORPORATIVA

- **Cumprimento:** atendimento às leis, regulamentos e acordos contratuais relacionados ao negócio;
- **Confiabilidade da informação:** prover a administração de informação, de modo a facilitar a operacionalidade da organização e dar credibilidade aos relatórios financeiros e responsabilidade da governança corporativa

MODELO DO PROCESSO

CobiT

- Incluir aqui quadro com modelo CobiT

PLANEJAMENTO E ORGANIZAÇÃO

- PO1 – Definir um plano estratégico de TI
- PO2 - Definir a arquitetura de informação
- PO3 - Determinar a direção tecnológica
- PO4 - Definir processos, organização e relacionamento da TI
- PO5 - Gerenciar o investimento em TI

PLANEJAMENTO E ORGANIZAÇÃO

- PO6 – Comunicar metas e diretivas gerenciais
- PO7 - Gerenciar recursos humanos
- PO8 - Garantir cumprimento de exigências externas
- PO9 - Avaliar riscos
- PO10- Gerenciar projetos
- PO11- Gerenciar qualidade

AQUISIÇÃO E IMPLEMENTAÇÃO

- AI1 – Identificar soluções
- AI2 - Adquirir e manter software aplicativo
- AI3 – Adquirir e manter arquitetura tecnológica
- AI4 – Desenvolver e manter procedimentos de TI
- AI5 – Instalar e certificar sistemas
- AI6 - Gerenciar mudanças

ENTREGA DOS SERVIÇOS

- DS1 – Definir níveis de serviços
- DS2 - Gerenciar serviços de terceiros
- DS3 - Gerenciar performance e capacidade
- DS4 – Garantir continuidade dos serviços
- DS5 – Garantir segurança dos sistemas
- DS6 – Identificar e alocar custos
- DS7 - Educar e treinar usuários

ENTREGA DOS SERVIÇOS

- DS8 – Auxiliar e aconselhar usuários de TI
- DS9 – Gerenciar a configuração
- DS10- Gerenciar problemas e incidentes
- DS11- Gerenciar dados
- DS12- Gerenciar instalações
- DS13- Gerenciar a operação

SUORTE E MONITORAMENTO

- M1 – Monitorar os processos
- M2 - Avaliar a adequação do controle interno
- M3 - Obter a certificação independente
- M4 - Prover a auditoria independente

OUTRAS VANTAGENS DO **CobiT**

- **Modelos de maturidade** para o controle dos processos de TI, permitindo a administração avaliar onde a organização está, como está perante seus concorrentes, como está em relação aos padrões internacionais e determinar como chegar lá

OUTRAS VANTAGENS DO CobiT

- **Fatores críticos de êxito** fixando as mais importantes diretrizes que devem ser consideradas pela administração, para ter controle sobre os processos de TI;
- **Indicadores chaves para lograr os objetivos e resultados(key goal indicators)**, que definem os mecanismos de medição que indicarão à administração se o processo de TI, já implantado, satisfaz os requerimentos do negócio

OUTRAS VANTAGENS DO **CobiT**

- **Indicadores chaves de desempenho (key performance indicators)** definem a medida para conhecer se o processo de TI está bem feito, comparado com os objetivos que a administração corporativa busca

OUTRAS VANTAGENS DO **CobiT**

- Dispõe de ferramentas de implementação usadas pelas empresas na aplicação do CobiT, tais como Diagnóstico de Sensibilização Gerencial e Diagnóstico de Controle de TI, que contêm as experiências vividas pelas organizações que adotaram o **CobiT** para análise do seu ambiente de TI.

O **CobiT** e a **SARBANES- OXLEY**

- Não existe na SOX menção voltada para TI
- Não existe nenhuma especificação de quais controles precisam ser estabelecidos dentro da TI para estar em conformidade com SOX
- As empresas estão adotando o **CobiT** como referencial pelo fato dele definir quais os objetivos de controle que precisam ser implementados em TI e também por ser um modelo independente de plataforma para avaliação de controle

PROCESSOS DO **CobIT** PARA SOX

- Processos que podem auxiliar na conformidade com a SOX
- 1) Adquirir e manter software aplicativo;
- 2) Adquirir e manter arquitetura tecnológica;
- 3) Desenvolver e manter procedimentos de TI
- 4) Instalar e certificar soluções e mudanças
- 5) Gerenciar mudanças;
- 6) Definir e gerenciar níveis de serviço;

PROCESSOS DO **CobIT** para SOX

- 7) Gerenciar serviços de terceiros;
- 8) Assegurar a segurança dos sistemas;
- 9) Gerenciar a configuração;
- 10) Gerenciar problemas;
- 11) Gerenciar dados;
- 12) Gerenciar operações.

DIRETRIZES DE AUDITORIA

- O **CobiT** possibilita aos auditores confrontar os processos de TI específicos com os objetivos da administração, para determinar onde os controles são suficientes ou onde podem ser aperfeiçoados, apresentando as recomendações para a sua melhoria

DIRETRIZES DE AUDITORIA

- As diretrizes de auditoria estão estruturadas para uma avaliação adequada dos controles internos da organização, a identificação das áreas de risco e o envolvimento da área de TI com os negócios da organização.

O PROCESSO DA AUDITORIA

- O processo da auditoria está dividido em quatro etapas:
- 1) Análise do ambiente empresarial e qualidade da administração;
- 2) Avaliação dos controles internos, abrangendo a área de TI;
- 3) Testes de Observância /conformidade
- 4) Testes Substantivos

AUDITORIA DE PROCESSOS

- Os requisitos para a auditoria de processos são os que seguem:
- 1) Definir o escopo da auditoria;
- 2) Enfoque com o processo do negócio;
- 3) Plataformas, sistemas e seus relacionamentos com o suporte ao processo;
- 4) Estrutura organizacional, funções e divisão de responsabilidades;
- 5) Identificar requisitos de informação relevantes para o processo do negócio;
- 6) Relevância para o processo do negócio;

AUDITORIA DE PROCESSOS

- 7) Identificar riscos inerentes de TI e um nível de controle abrangente;
- 8) Mudanças recentes e incidentes no negócio e ambiente de TI;
- 9) Resultados de auditorias auto-avaliações e certificações;
- 10) Controles de monitoramento adotados pela administração;
- 11) Selecionar processos e plataformas a serem auditadas

METODOLOGIA DA AUDITORIA DE PROCESSOS

- Avaliação dos controles internos e das áreas de riscos;
- Etapas do trabalho, abrangência dos exames e definição dos procedimentos de auditoria;
- Pontos de deficiências levantados
- Recomendações para a melhoria dos sistemas

RESUMINDO OS BENEFÍCIOS

- Melhor alinhamento, baseado no foco dos negócios;
- Uma visão ampla sobre o impacto da TI na organização;
- Responsabilidades e propriedades baseadas na orientação de processos;
- Condições de avaliar o retorno dos investimentos em TI;
- Entendimento compartilhado com todos os interessados, numa linguagem comum;
- Cumprimento dos requerimentos internacionais parao ambiente de controle de TI

CONTATOS

- Antonio Carlos Nasi
- Tel. (51) 3342 9388
- E-mail: nasi@nardonnasi.com.br

- Carlos Renato Maia
- Tel. (51) 3342 9388
- E-mail: maia@nardonnasi.com.br