AUDITORIA DE SISTEMAS

FACULDADE DE ECONOMIA, ADMINISTRAÇÃO E CONTABILIDADE
DE RIBEIRÃO PRETO
UNIVERSIDADE DE SÃO PAULO

DISIPLINA: AUDITORIA E PERÍCIA

DOCENTE: PAULA CAROLINA C. NARDI

ISADORA R. C. LIMA
LETÍCIA DE O. CONSTANTINO
NATÁLIA ZAMBON

INTRODUÇÃO

ERP – HISTÓRICO

FERRAMENTAS E PROCESSOS DE ANÁLISES DE DADOS

AUDITORIA DE SISTEMAS

CASOS PRÁTICOS

ENTERPRISE RESOURCE PLANNING - ERP

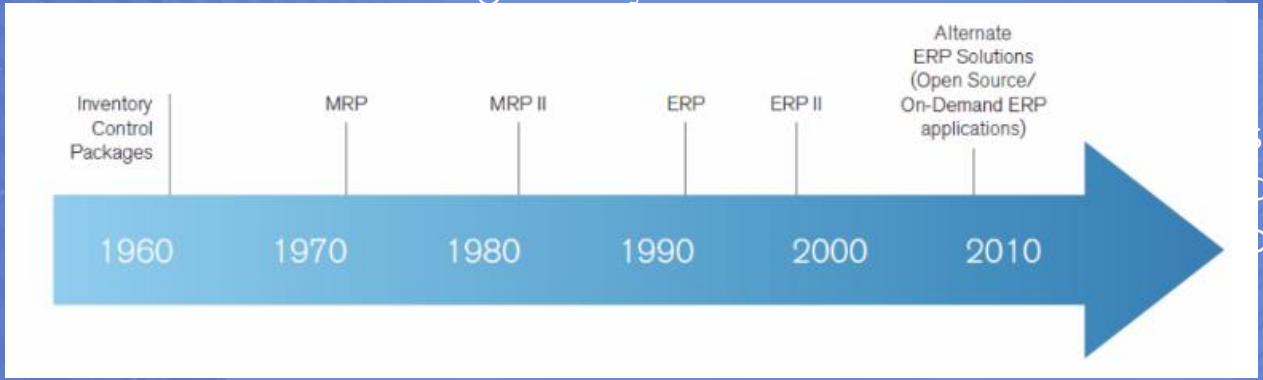
ENTERPRISE RESOURCE PLANNING - ERP

Contexto

> Mainframes para controles de estoque (1950);

> MRP - Material Requirement Planning (1960 e 1970): permite a gestão e o controle dos inventários;

> ERP - Enterprise Resource Planning (década de 90): foi possível integrar as áreas de recursos humanos, vendas, marketing, finanças, faturamento, contabilidade, entre



da de

o de

ENTERPRISE RESOURCE PLANNING - ERP

Importância

> Mostram dados em Tempo Real através de relatórios

> Informações que se interagem e se alimentam

> Auxiliam na tomada de de Decisão

> *Supplychain*

ENTERPRISE RESOURCE PLANNING - ERP

Prós

> Elimina Uso de Interfaces Manuais
> Elimina retrabalho
> Aprimoramento dos processos internos
> Informação de qualidade em tempo real
> Otimiza tomada de decisão
> Melhor gestão dos resultados

Contras

> Altos custos de implementação
> Dependência do fornecedor
> Dependência da Tecnologia
> Mão-de-obra capacitada
> Padronização entre as empresas do segmento

AUDITORIA DE SISTEMAS

É a avaliação e a validação do controle interno de sistemas de informação

AUDITORIA DE SISTEMAS

Histórico

> Utilização crescente de Sistemas de Gestão
> Necessidade de melhor gerenciamento e criação de controles

Objetivos

> Validar e avaliar os controles internos de Sistemas
> Validar a eficácia do sistema
> Reunir, agrupar e validar evidências
> Garantir a segurança (física e lógica) da Informação e sistema

Segurança da Informação

> Integridade
> Disponibilidade
> Confidencialidade

AUDITORIA DE SISTEMAS

Extras

Pode detectar problemas em:

> Fraudes em e-mail;

> Uso inadequado de hardwares;

> Fraudes, erros e acidentes;

> Vazamento de informações;

> Falta de segurança física (acessos indevidos;

AUDITORIA DE SISTEMAS

Auditoria de TI ≠ Auditoria de Controles por meio de TI

Auditoria de TI	Auditoria de controles por meio de ferramentas de TI
Exemplo de teste de auditoria: Verificação controles de acesso para alteração da base de dados de um ERP (alto risco)	Exemplo de teste de auditoria: Verificação de acessos para testes de segregação de função
Mais realizados por externas e auditorias especializadas	Mais realizado por auditorias internas (externas com foco nas DC's)

AUDITORIA DE SISTEMAS

Tipos de abordagem de auditorias de sistemas

> Ao redor do computador:

Trabalha com documentos de entrada e saída;

Não necessita profundo conhecimento em TI;

- **Vantagens:** baixo custo
- **Desvantagens**: Incompleta, poucos parâmetros

> Através do computador:

Envolve aprovação e registro de transações;

Utiliza técnicas de verificação;

Vantagens: aprofundado validação e apontamentos;

Desvantagens: alto custo

AUDITORIA DE SISTEMAS

Principais tipos de auditorias de sistemas

> Auditoria Legal ou Regulatória: Atendimento a regulamentações locais e internacionais (Lei Sarbanes-Oxley, Basileia II, Comissão de Valores Mobiliários, etc).

> Auditoria de Integridade de Dados: Classificação dos dados, atualização, bancos de dados, aplicativos, acessos, estudo dos fluxos (entradas e saídas) de transmissão, controles de verificação qualidade e confiabilidade das informações. (exemplo anexo)

> Auditoria em Segurança da Informação: Métodos de autenticação, autorização, criptografia, gestão de certificados digitais, segurança de redes, gestão dos usuários, configuração de antivírus, atualizações, políticas, normas, manuais operacionais.

AUDITORIA DE SISTEMAS

Principais tipos de auditorias de sistemas

> Auditoria de Segurança Física: Avaliação de localidades e riscos ambientais: vidas (capital intelectual), furto/roubo, acesso, umidade, temperatura, acidentes, desastres, etc. e as proteções: perímetros de segurança, câmeras, sensores, guardas, dispositivos, proteções do ambiente.

> Auditoria de Desenvolvimento de Sistemas: Validação dos processos de gestão de projetos, cumprimento de metodologia de qualidade, orçamentos previstos e realizados e avaliação de desvios.

AUDITORIA DE SISTEMAS

Por que ter uma auditoria de sistemas?

> Para ter transparência na área de TI e processos da empresa

> SOX (30/07/2002)

AUDITORIA DE SISTEMAS

O processo de certificação do auditor de sistemas

> CISA – Certified Information Systems Auditor

> Oferecida pelo ISACA

> Uma das mais reconhecidas e eficazes em âmbito global

AUDITORIA DE SISTEMAS

O processo de certificação do auditor de sistemas

> Para passar no exame:

Demonstrar experiência e qualificações profissionais, fornecer evidência de práticas; aderir formalmente ao código de ética do ISACA, etc.

> Para manutenção do certificado:

Participar de atividades educacionais e comprovar que contribuiu para a profissão de auditori de maneira “correta”

AUDITORIA DE SISTEMAS

O processo de certificação do auditor de sistemas

> Para passar no exame:

Demonstrar experiência e qualificações profissionais, fornecer evidência de práticas; aderir formalmente ao código de ética do ISACA, etc.

> Para manutenção do certificado:

Participar de atividades educacionais e comprovar que contribuiu para a profissão de auditori de maneira “correta”

AUDITORIA DE SISTEMAS

O CIO (Chief Information Officer

> Profissão que contempla o papel principal de fomentar a capacitação da organização necessária para extrair um maior valor dos investimentos em TI. O CIO é um participante crítico, considerando a crescente importância de TI na ativação do desempenho e da competitividade dos negócios. O CIO passou de gerente funcional para gerente geral com escopo e responsabilidades de toda a empresa.

AUDITORIA DE SISTEMAS

QOS – Quality Of Service

> Imposição de requisitos de qualidade no momento da aquisição do serviço, em:
>> Sistema de manufaturas;
>> Sistema de compensação bancária;
>> Plataformas de telecomunicação, etc.

> O objetivo é reduzir custos, simplificar a manutenção e facilitar a interoperabilidade do sistema

AUDITORIA DE SISTEMAS

EDP – Electronic Data Processing

> Processamento de dados que é realizado através de dispositivos eletrônicos, que, segundo a norma NPC T 11:

>> modifica a forma de processamento e armazenamento de informações, afetando a organização e os procedimentos adotados pela entidade na consecução de adequados controles internos;

>> julga importante conhecer suficientemente o sistema de contabilidade e controle interno afetado pelo ambiente de PED;

deve determinar o efeito que o ambiente de PED possa ter sobre a avaliação de risco global da entidade em nível de saldos de contas;

>> estabelecer e supervisionar o nível de provas de controle e de procedimentos substantivos capaz de assegurar a confiabilidade necessária para conclusão dos controles internos e das demonstrações contábeis.

ANÁLISE DE DADOS E FERRAMENTAS

AUDITORIA DE SISTEMAS

CAAT – Computer Aided Audit Tools

> A CAAT ou TAACs - Técnicas de Auditoria Auxiliadas por Computador - são técnicas ou programas de computador especializados para gerar amostras, importar dados, sumarizar e testar os controles, condições e processos implantados nos sistemas através das amostras que selecionamos.

CAAT – Computer Aided Audit Tools

ANÁLISE DE DADOS E FERRAMENTAS

> **Software Especializado para Auditoria (SEA)**
Permite ao auditor realizar testes em arquivos e bancos de dados.
Ex.: ACL, IDEA, etc.

> **Software de Auditoria Adaptado (SAA)**
Geralmente desenvolvidos por auditores para desempenhar tarefas específicas, são necessários quando os sistemas da empresa não são compatíveis aos SEA, ou quando o auditor quer realizar testes não possíveis com os SEA.
Ex.: Easy Trieve, SQL+, SAS, etc

CAAT – Computer Aided Audit Tools

ANÁLISE DE DADOS E FERRAMENTAS

> **Teste de Dados ou Recálculo de Operações**
O auditor testa os dados para verificar os controles empregados no sistema através de validação nestes dados> **Simulação em Paralelo**
O auditor utiliza as informações do sistema para mapear e construir os passos a serem simulados em outra ferramenta a fim de chegar ao mesmo resultado do sistema.
> **Testes integrados**
O auditor submete parâmetros de teste com dados reais, sem impactar na rotina normal de processamento do sistema.

ITIL - Information Technology Infrastructure Library

ANÁLISE DE DADOS E FERRAMENTAS

> Criação

Final dos anos 80 pela CCTA (Central Computer and Telecommunications Agency), hoje OGC (Office for Government Commerce) da Inglaterra

> Características

Gestão com foco no cliente e na qualidade dos serviços de tecnologia da informação (TI)

ITIL - Information Technology Infrastructure Library

ANÁLISE DE DADOS E FERRAMENTAS

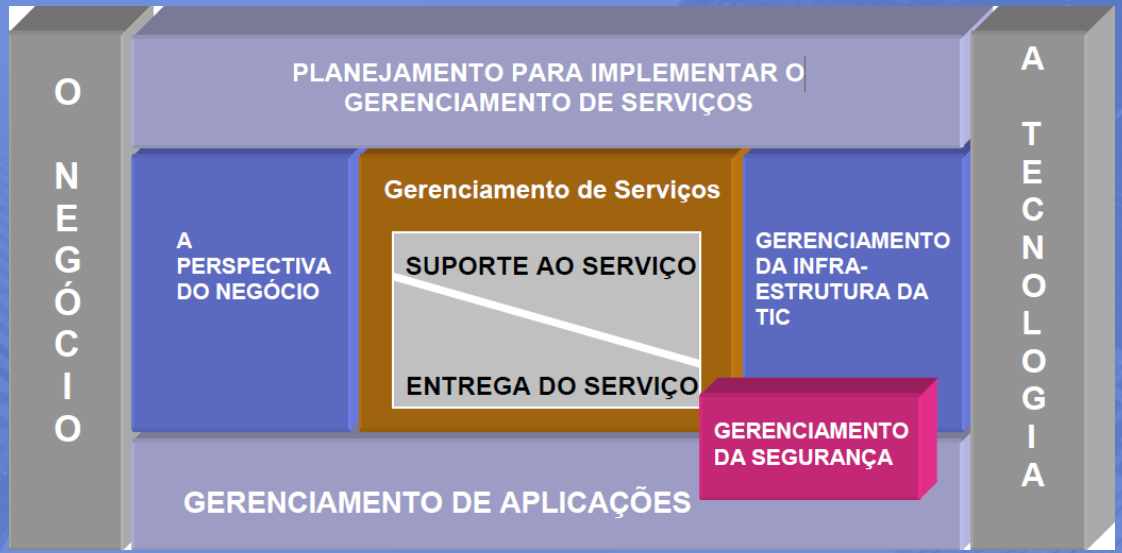
> Conjunto de padrões que provê os fundamentos para o processo de gerenciamento dos recursos tecnológicos da TI.

> Apresenta uma abordagem prática dos processos de produção e entrega dos serviços

> Na Gestão de Segurança, o ITIL possui um processo específico para a Segurança da Informação, enfatizando a importância do adequado gerenciamento da SI..

ANÁLISE DE DADOS E FERRAMENTAS

ITIL - Information Technology Infrastructure Library



ANÁLISE DE DADOS E FERRAMENTAS

ITIL - Information Technology Infrastructure Library

Resultados

> Fortalecimento dos Controles e da Gestão
> Orientação a processos
> Diminuição gradativa da indisponibilidade
> Elevação dos níveis de satisfação
> Redução dos custos operacionais

ANÁLISE DE DADOS E FERRAMENTAS

COBIT – Control Objectives for Information and related Technology

> Trata-se de um framework focado na governança de TI, que é mantido pelo ISACA, um instituto de atuação internacional formado por diversas empresas de TI ao redor do globo e que gere certificações de segurança, auditoria, governança e risco internacionalmente reconhecidas.

Missão: “Pesquisar, desenvolver, publicar e promover um conjunto de objetivos de controle para tecnologia que seja embasado, atual, internacional e aceito em geral para o uso do dia-a-dia de gerentes de negócio e auditores.” Fonte: ISACA

ANÁLISE DE DADOS E FERRAMENTAS

COBIT – Control Objectives for Information and related Technology

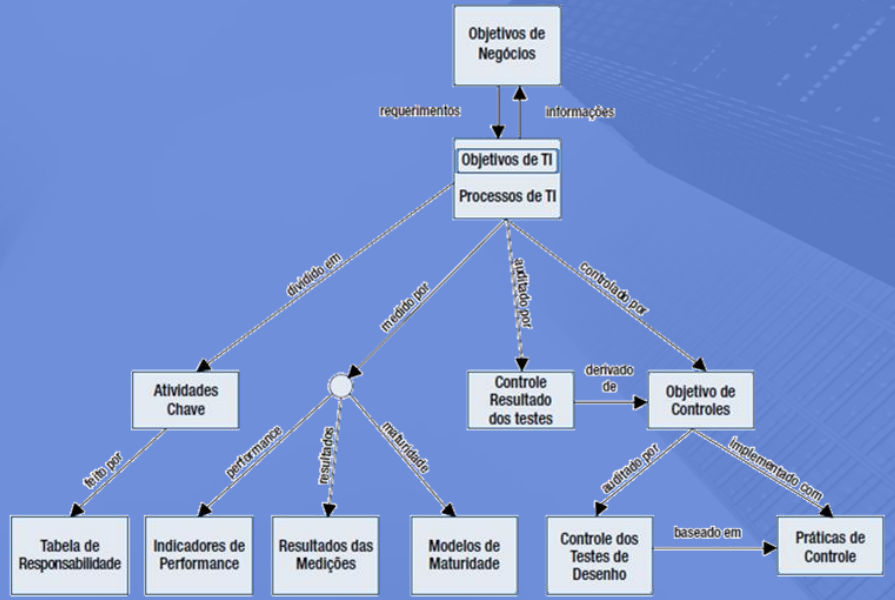
> Inicialmente, o framework aplica uma série de práticas envolvendo etapas do planejamento ao monitoramento dos resultados e métricas. A partir da avaliação dessas etapas, o COBIT começa a detectar e estabelecer quais são as práticas mais adequadas em governança de TI que trabalhem em consonância com a realidade e objetivos da empresa.

Em seguida, são descritos os processos e definidos os objetivos de controle específicos, pertinentes à realidade e necessidades do empreendimento. A avaliação das etapas e processos funcionará, ainda, como um auxílio na correção de não-conformidades. Isto ajudará na divisão e delegação de tarefas e na avaliação do nível de interação entre os processos.

ANÁLISE DE DADOS E FERRAMENTAS

COBIT – Control Objectives for Information and related Technology

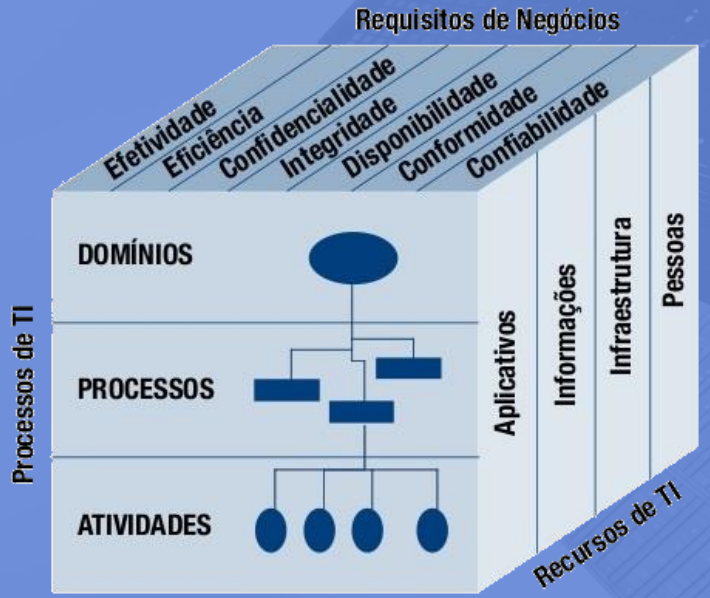
Inter-relacionamento do componentes de COBIT



ANÁLISE DE DADOS E FERRAMENTAS

Como os componentes se relacionam

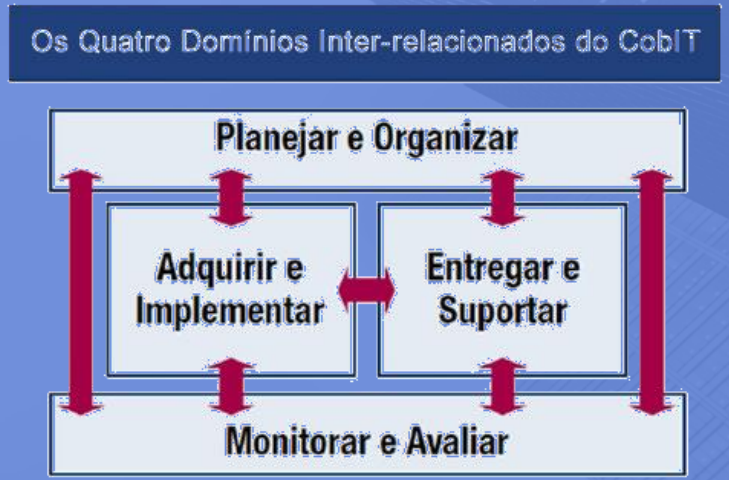
COBIT – Control Objectives for Information and related Technology



ANÁLISE DE DADOS E FERRAMENTAS

COBIT – Control Objectives for Information and related Technology

Objetivos de controle separados em 34 processos agrupados em 4 domínios



ANÁLISE DE DADOS E FERRAMENTAS

COBIT x ITIL

> Níveis estratégicos e de controle
> Priorizar e controlar os processos de gestão e governança
> O QUE fazer

> Níveis operacionais e táticos
> Modelar e executar processos escolhidos
> COMO fazer

ANÁLISE DE DADOS E FERRAMENTAS

Os riscos e controles + Conceitos sobre COSO

> COSO – *Comittee of Sponsoring Organizations of Treadway Commission*
Criada em 1985 para estudar fraudes
Formado por membros das 5 maiores associações contábeis americanas:

> *American Accounting Association (AAA);*
> *American Institute of Certified Public Accountants (AICPA);*
> *Financial Executives International (FEI);*
> *Institute of Internal Auditors (IIA);*
> *Institute of Management Accountants (IMA).*

ANÁLISE DE DADOS E FERRAMENTAS

Os riscos e controles + Conceitos sobre COSO

> O que é risco?

Risco, generalizadamente, é tudo aquilo que pode impedir a companhia de alcançar **objetivos** de maneira correta.

> O que é controle interno?

Processo afetado pela direção da entidade e outros membros, desenvolvido para prover segurança razoável do alcance de **objetivos** operacionais, de divulgação e *compliance*.

ANÁLISE DE DADOS E FERRAMENTAS

Relação COSO e COBIT

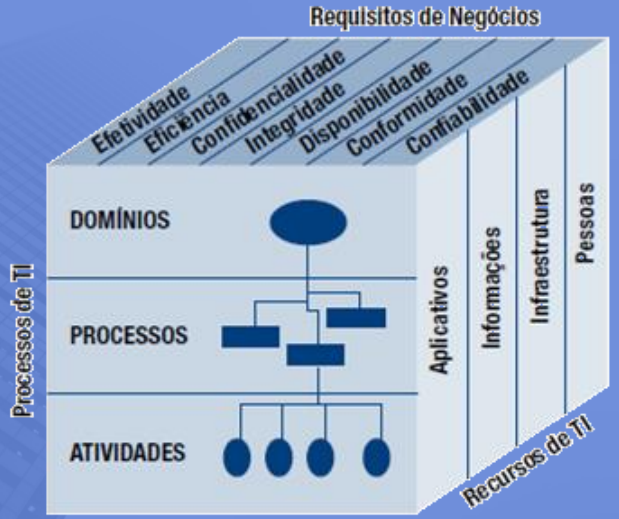
> Tendo Lançado o COBIT 5 em Abril de 2012, a ISACA participou da formulação do novo Framework COSO como membro do Conselho de Consultivo;
> *"Não é possível avaliar a eficácia dos controles internos de uma organização sem garantir a conformidade dos sistemas de informação"*;
> Função de Suporte ao Framework COSO – complementar; COBIT é o modelo de controles internos mais utilizado para TI;
> O novo Framework do COSO (2013) dá uma ênfase muito maior à importância da TI para controles internos.

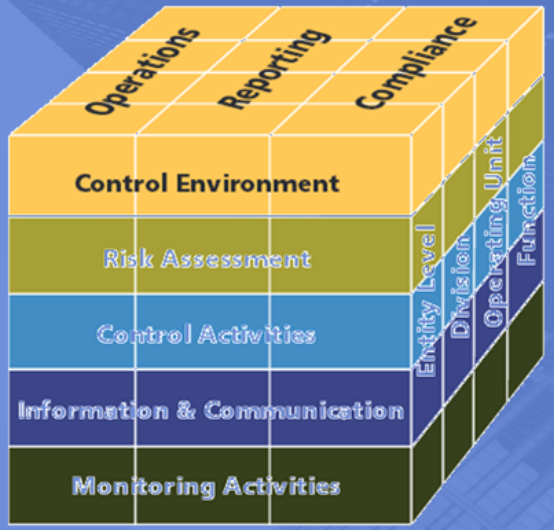
.

ANÁLISE DE DADOS E FERRAMENTAS

Principais *framewoks de COBIT x COSO*

Relação COSO e COBIT





How COSO Framework Control Environment Principles Relate to COBIT 5 Framework Components and Content

COSO Principle[11]	COBIT 5 Relationship to COSO Principle
"1. The organization demonstrates a commitment to integrity and ethical values."	The COBIT 5 Culture, Ethics and Behaviour enabler addresses enterprise ethics and individual ethics and behaviors, including risk taking, by following policy and addressing negative outcomes. The COBIT 5 processes EDM01 *Ensure governance framework setting and maintenance* and APO01 *Manage the IT management framework* include activities to embed enterprise integrity and ethical value aspects within the governance and management framework. The COBIT 5 process APO07 *Manage human resources* includes activities to address integrity and ethical value aspects from a human resources perspective.
"2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control."	The COBIT 5 principle Separating Governance from Management supports the second COSO principle by differentiating governance and management disciplines and making independence easier to establish and maintain. In addition, all five COBIT 5 governance processes (EDM01 through EDM05) reinforce this separation in their RACI chart guidance.
"3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives."	The COBIT 5 Organisational Structure enabler addresses practices, such as operating principles, span of control (scope) definition, level of authority, delegation of authority powers and escalation paths, to support the establishment of effective organizational structures within enterprises. COBIT 5 process APO01 *Manage the IT management framework* includes activities to address the required definition of an organizational structure for the enterprise. APO01 takes direction from COBIT 5 process EDM01 *Ensure governance framework setting and maintenance* in respect to enterprise governance requirements.
"4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives."	The COBIT 5 People, Skills and Competencies enabler addresses the life cycle aspects that are related to people—knowing the current skills base; the skills that need to be retained, developed or acquired to meet enterprise goals; and the skills that can be disposed of when no longer needed. COBIT 5 process APO01 *Manage the IT management framework* includes activities to establish roles and responsibilities to support achievement of enterprise objectives. COBIT 5 process APO07 *Manage human resources* includes activities to address the attraction, development and retention of competent people.
"5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives."	The COBIT 5 Processes enabler and the RACI charts that support the 37 processes are particularly relevant in the context of individual accountability. The enabler and charts strongly advocate the assignment of responsibilities and accountabilities and provide examples of roles and responsibilities for the individual and group roles for all key GEIT-related processes and activities.

ANÁLISE DE DADOS E FERRAMENTAS

Relação COSO e COBIT

> Os *frameworks* são complementares e compatíveis como direcionadores para facilitar o estabelecimento e o desenvolvimento de práticas e atividades de controle interno dentro da estrutura de governança de uma entidade.

> O *framework* COSO fornece valiosos princípios de controle interno, enquanto o COBIT 5 constitui uma direção sobre os métodos de governança de TI mais críticos na utilização de controles financeiros internos de empresas

.

ANÁLISE DE DADOS E FERRAMENTAS

Relação COSO e COBIT

> Os *frameworks* são complementares e compatíveis como direcionadores para facilitar o estabelecimento e o desenvolvimento de práticas e atividades de controle interno dentro da estrutura de governança de uma entidade.

> O *framework* COSO fornece valiosos princípios de controle interno, enquanto o COBIT 5 constitui uma direção sobre os métodos de governança de TI mais críticos na utilização de controles financeiros internos de empresas

.

CASOS PRÁTICOS

BANCO CENTRAL

> Uso do COBIT pela auditoria interna;
> Utiliza como um guia para a avaliação das instituições financeiras bancárias e não bancárias;
> Elaboração de uma matriz que relaciona o grau de importância do processo para a organização com o grau de confiança da auditoria nos controles desses processos;
> É encaminhada para a controladoria geral da união para avaliação.

.

BANCO CENTRAL

> É feito um questionário de avaliação do Controle Interno de TI, com questões objetivas;
> Essas questões são classificadas em: ambiente de controle, gerenciamento de riscos, atividade de controle, comunicação e informação e monitoramento;
> Ao final da aplicação do questionário, a auditoria conclui sobre a adequação do controle interno para a atividade examinada: ótimo, bom, regular, deficiente ou precário.

BANCO CENTRAL

> As recomendações são acompanhadas pela Auditoria, e os prazos para a conclusão das providencias é combinado com a unidade recomendada.
> No vencimento do prazo, a unidade recomendada deve informar a auditoria sobre a conclusão, o andamento ou a motivação do atraso para a conclusão do plano de ação.
> Quadrimestralmente o auditor deve prestar informações a diretoria colegiada sobre o cumprimento das recomendações

.

BRASKEM

> Braskem – Grupo de empresas que atuam no setor químico e petroquímico.
> Destaca-se como a maior produtora de resinas termoplásticas das américas.
> Empresa de capital aberto.
> Estratégia com o uso da metodologia do COBIT
> Crescimento baseado na aquisição de empresas
Integrar operações e garantir o processo de governança corporativa em TI

.

BRASKEM

> A Braskem avaliou e mapeou o grau de maturidade de cada um de seus processos;
> Durante quatro semanas, a Ci&T analisou a área de tecnologia da > Braskem com base no Cobit;
> Pegou-se os processos mais críticos, que tinham o maior impacto sobre a estratégia da empresa;
> Uma das áreas mais importantes nesse processo de análise foi a de gerenciamento de projetos;
> A decisão de implementar o Cobit e contratar a Ci&T ajudou a Braskem a planejar suas ações de TI em 2009;

BRASKEM

> Houve três grandes objetivos na adoção do CobiT: primeiro, a área de TI dar uma garantia de suporte ao negócio com qualidade; o segundo, colocar à prova a prontidão do departamento de TI para atender a estratégia de crescimento da Braskem; e o terceiro, melhorar a performance dos processos de negócio da empresa;
> A Braskem decidiu criar um escritório de gerenciamento de projetos (PMO), que entrou em operação no último trimestre do ano passado e, como consequência, primeiro, os projetos tiveram melhor controle de orçamento, de riscos, de prazo e de qualidade e, segundo, diminuíram as incidências de projetos que começaram atrasados e com baixa qualidade;
> Foi organizada também uma área de governança de processos, com membros das áreas de TI e de negócios junto com o PMO;

.

OBRIGADA!

FONTES & REFERÊNCIAS