VII Encontro de Auditoria e Unidades de Controle Interno do Sistema "S"

Auditoria Interna e Governança

Controladoria Geral da União - CGU

Atuação da Auditoria Interna na Avaliação da Gestão de Tecnologia da Informação

Emerson de Melo

Brasília – Novembro/2011

Principais Modelos de Referência para Auditoria de TI

Como focar no negócio da Instituição com direcionamento preventivo de ações na área de governança da informação e atender os órgãos de controle?

Público-Alvo da Apresentação

- Gerentes e Diretores das Entidades
- Gerentes e Diretores das áreas de TI
- Auditores
- Profissionais da Área Técnica
- Analistas de Negócio

Conteúdo da Apresentação

1.Conceitos (Controle Interno, Auditoria governamental, Auditoria Anual de Contas Auditoria de Sistemas, Governança)

2.Cenário atual da Auditoria de Sistemas

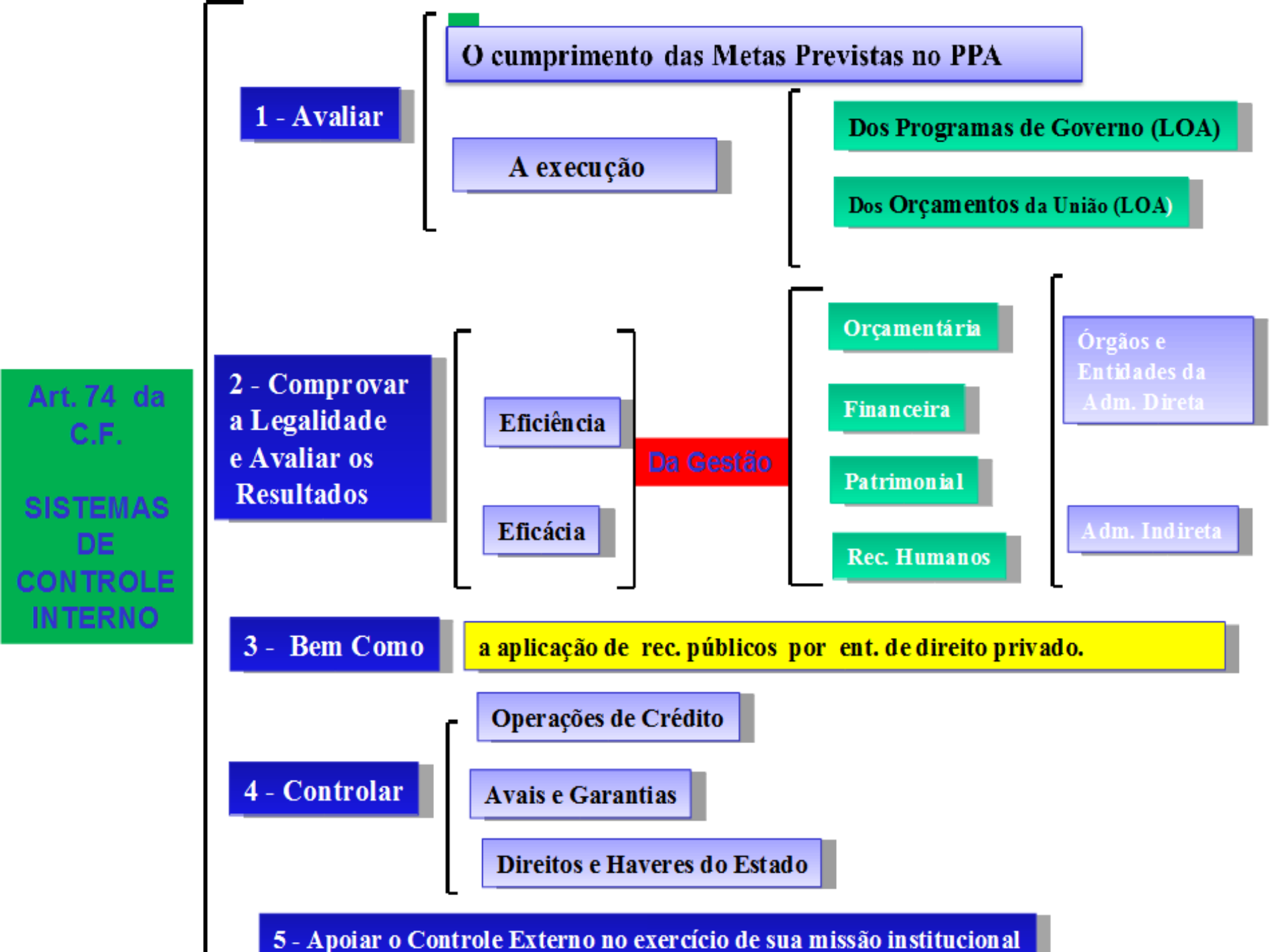
3.Principais Modelos de Referência para Auditoria de Sistemas

4.O principal Modelo de Referência de Auditoria “COBIT”

5.O novo modelo de avaliação da gestão (tópicos de TI)

6.Normativos da área de auditoria de TI

7.Ações levantamento de TI no sistema “S”


Art. 74 da C.F.
SISTEMAS DE CONTROLE INTERNO
1 - Avaliar
O cumprimento das Metas Previstas no PPA
A execução
Dos Programas de Governo (LOA)
Dos Orçamentos da União (LOA)
2 - Comprovar a Legalidade e Avaliar os Resultados
Eficiência
Eficácia
Da Gestão
Orçamentária
Financeira
Patrimonial
Rec. Humanos
Órgãos e Entidades da Adm. Direta
Adm. Indireta
3 - Bem Como
a aplicação de rec. públicos por ent. de direito privado.
4 - Controlar
Operações de Crédito
Avais e Garantias
Direitos e Haveres do Estado
5 - Apoiar o Controle Externo no exercício de sua missão institucional

Auditoria Anual de Contas

- A Auditoria Anual de Contas visa instrumentalizar o Tribunal de Contas da União para o julgamento das contas dos administradores públicos.

- O desenvolvimento deste trabalho também permite à CGU acompanhar e avaliar a gestão dos administradores públicos federais, contribuindo para a melhoria da gestão pública.

Fonte www.cgu.gov.br

- Lei Nº 8.443/92 - Lei Orgânica TCU.

Art. 5° A jurisdição do Tribunal abrange:

(...)

V - os responsáveis por **entidades dotadas de personalidade jurídica de direito privado** que recebam contribuições **parafiscais** e prestem serviço de **interesse público ou social**;

Auditoria Governamental

Constitui-se a Auditoria Governamental no conjunto de **técnicas e procedimentos** desenvolvidos com vistas a **avaliar a aplicação e gestão dos recursos públicos** por parte das entidades integrantes da administração pública direta e indireta, **assim como das entidades de direito privado que administrem recursos públicos.**

Auditoria de Sistemas de Informação

Auditoria de Sistemas de Informação é "a revisão dos sistemas de informação, para verificar se realizam as funções e operações para as quais foram criados, assim como comprovar se os dados e demais informações neles contidos correspondem aos princípios de confiabilidade, integridade, precisão e disponibilidade".

Fonte: Intervención General de la Administración del Estado (IGAE)

Governança de TI

"É de responsabilidade da alta administração (incluindo diretores e executivos) na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização.

Fonte : IT governance Institute

AUDITORIAS EM TI
CENÁRIO ATUAL

CGU

-Mudança no foco de atuação das auditorias tradicionais

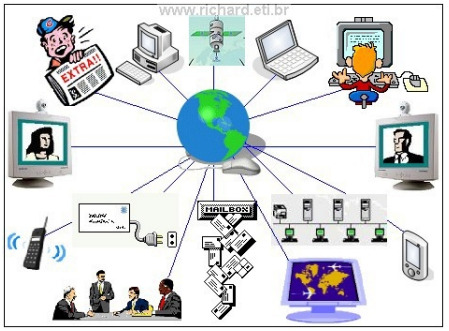
-Contratação de servidores da área de TI (SFC)

-Criação da SEFIT (TCU)

-Auditorias com foco em TI em órgãos da Administração Direta e Indireta pela CGU

-Construção de Acórdãos e Levantamentos da área de Tecnologia da Informação pelo TCU

COMO AUDITAR A ÁREA DE TECNOLOGIA ??



Principais Modelos de Referência para Auditoria de TI

COBIT

- Control OBjectives for Information and related Tecnology

-"Objetivos de controle para informação e tecnologia relacionada"

O COBIT inclui recursos tais como:

- sumário executivo (guia gerencial)
- framework (estrutura das áreas de controle)
- objetivos de controle (34 objetivos>>318 procedimentos)
- mapas de auditoria
- guia com técnicas de gerenciamento (guia técnico)

Principais Modelos de Referência para Auditoria de TI

NBR ISO/IEC 27002/2005

Estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de **segurança da informação** em uma organização.

ABNT NBR 15999-1:2007

Código de boas práticas para a **gestão de continuidade de negócios**

INOVAÇÕES DOS NORMATIVOS DO TCU NA ÁREA DE TI

A partir de 2011, a avaliação da gestão das entidades e órgãos jurisdicionados aos órgãos de controle foram **alvo de análise de aspectos de tecnologia da informação.**

Com base nos resultados das auditorias surgiu a necessidade de sistematizar anualmente essa avaliação da área tecnológica.

- Decisão Normativa TCU nº 108/2010, ANEXO II
- Portaria CGU nº 2.546, de 27 de dezembro de 2010

Decisão Normativa TCU nº 108/2010, ANEXO II, item 12

Informações sobre a gestão de tecnologia da informação (TI) da UJ, contemplando os seguintes aspectos:

a) Planejamento da área;
b) Perfil dos recursos humanos envolvidos;
c) Segurança da informação;
d) Desenvolvimento e produção de sistemas;
e) Contratação e gestão de bens e serviços de TI.

Área de Exame: SISTEMA DE INF. OPERACIONAIS

A) PLANEJAMENTO ESTRATÉGICO DE TI

I - Objetivo:

Verificar a **existência de Planejamento Estratégico de Tecnologia de Informação** alinhado às necessidades da Unidade e ao cumprimento de sua missão institucional.

B) POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

I - Objetivo:

Avaliação objetiva sobre a gestão de TI da unidade, no que diz respeito à salvaguarda da informação, em especial para as seguintes questões:

a) **Política de Segurança da Informação** (PSI); e
b) Verificação **de uma área específica**, com responsabilidades definidas, para lidar estrategicamente com segurança da informação.

C) RECURSOS HUMANOS DE TI

I - Objetivo:

Verificar a estrutura de pessoal de Tecnologia da Informação da Entidade, **identificando o perfil dos recursos humanos de TI envolvidos**, a distribuição desses recursos entre **funcionários e terceirizados** e a existência de **carreiras específicas** para a área de TI no plano de cargos da Entidade.

D) DESENHO E PRODUÇÃO DE SISTEMAS

I - Objetivo:

Verificar a existência e a adequação de **metodologia de desenvolvimento de sistemas utilizada no setor de informática da Unidade Jurisdicionada**; a existência de avaliações de rotina para verificação de **compatibilidade** entre os recursos de TI e as necessidades da UJ; e a existência de gestão de **acordos de níveis de serviço** das soluções de TI.

E) CONTRATAÇÕES E GESTÃO DE AQUISIÇÃO DE TI

I – Objetivo:

Verificar se as **contratações e Gestão de Bens e Serviços de TI são executados em consonância com o PDTI** e normas legais, após análise das necessidades da entidade, garantindo uma aquisição eficiente e eficaz, que contribua com o alcance da missão institucional.

Principais Modelos de Referência para Auditoria de TI

- COBIT

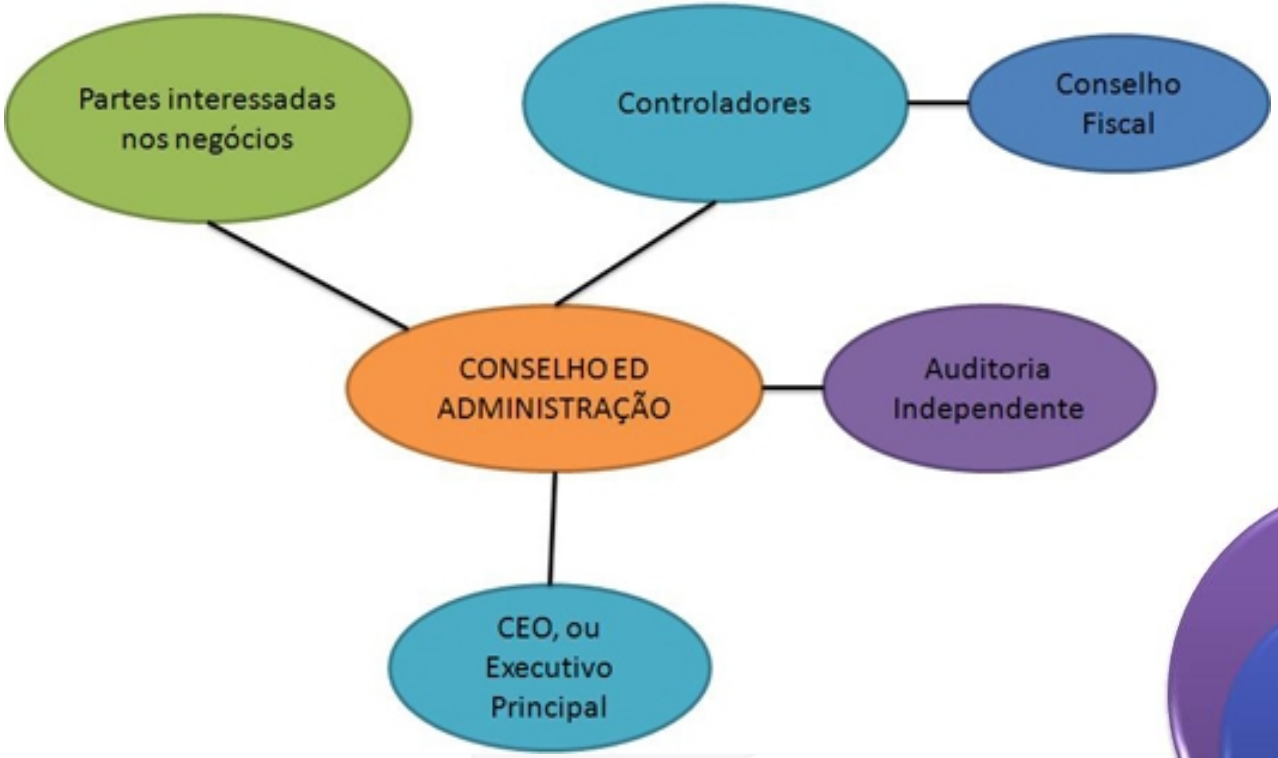
- É um Guia para a gestão de TI recomendado pelo ISACF (Information Systems Audit and Control Foundation, www.isaca.org).

- É o mais utilizado pelas empresas, órgãos e entidades de auditoria como referência mundial.

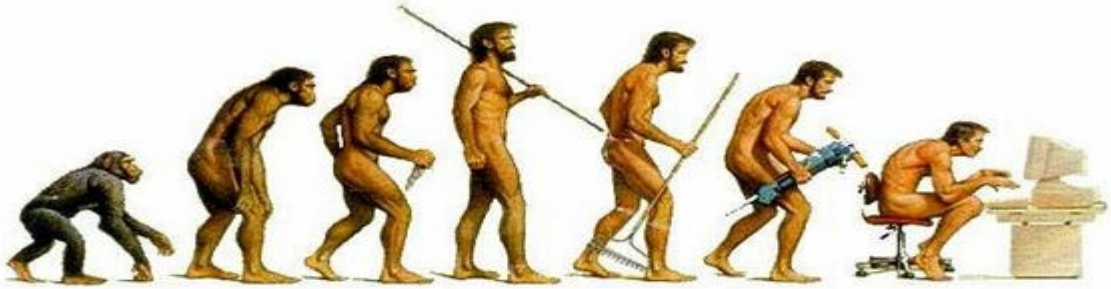
- O framework possui um mapeamento das **áreas e processos críticos de sucesso** para uma boa governança de TI.

COBIT

Sistema de Governança Corporativa



COBIT



EVOLUÇÃO DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

TI COMO PROVEDOR DE SERVIÇOS	TI COMO PARCEIRO ESTRATÉGICO
TI é separada do negócio	TI é inseparável do negócio
TI é vista como um gasto a controlar	TI é vista como um investimento a gerenciar

COBIT

Desafios da TI

-Alinhar TI ao Negócio

-Entregar valor (não frustar usuários)

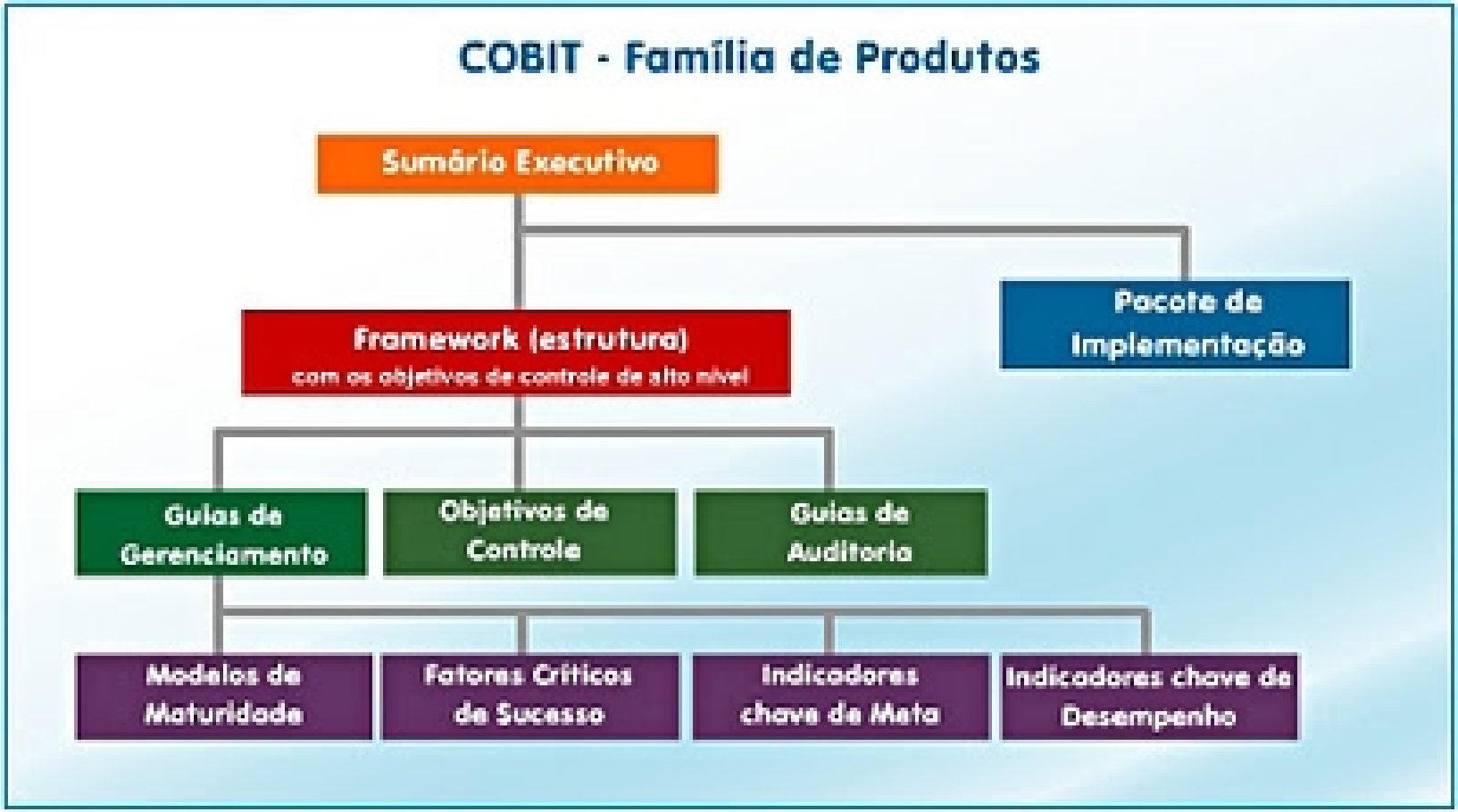
-Demonstrar ROI (Return Over Investiment)

-Gerenciar Segurança

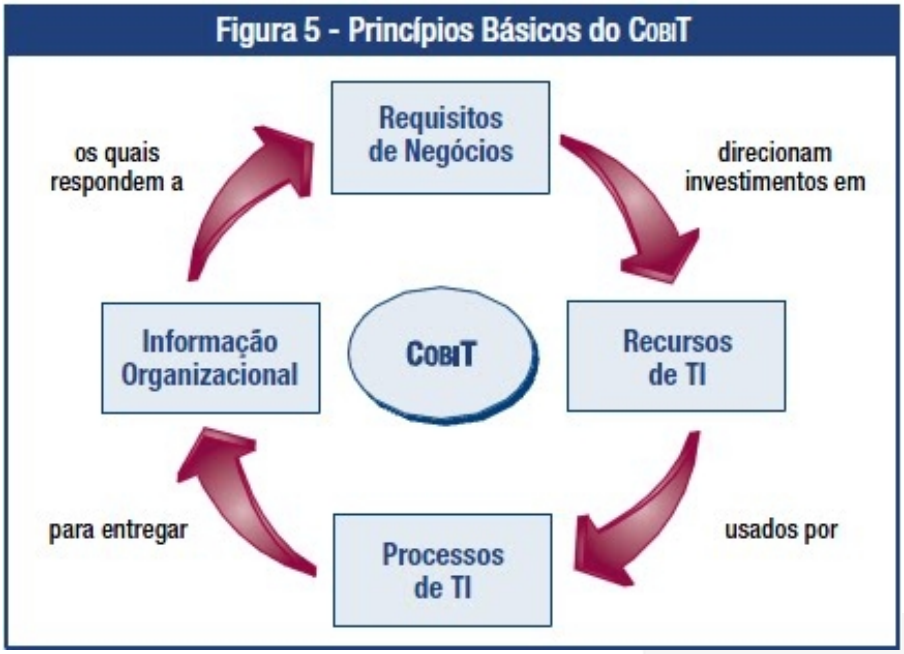
-Reduzir custos

-Envolver as partes interessadas (stakeHolders)

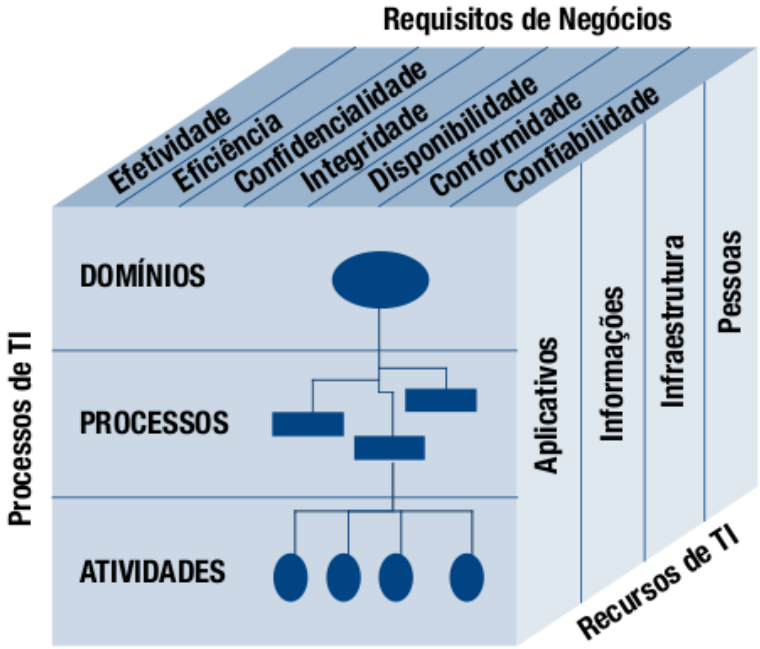
Principais Modelos de Referência para Auditoria de TI



Principais Modelos de Referência para Auditoria de TI - COBIT



CONCEPÇÃO DO MODELO



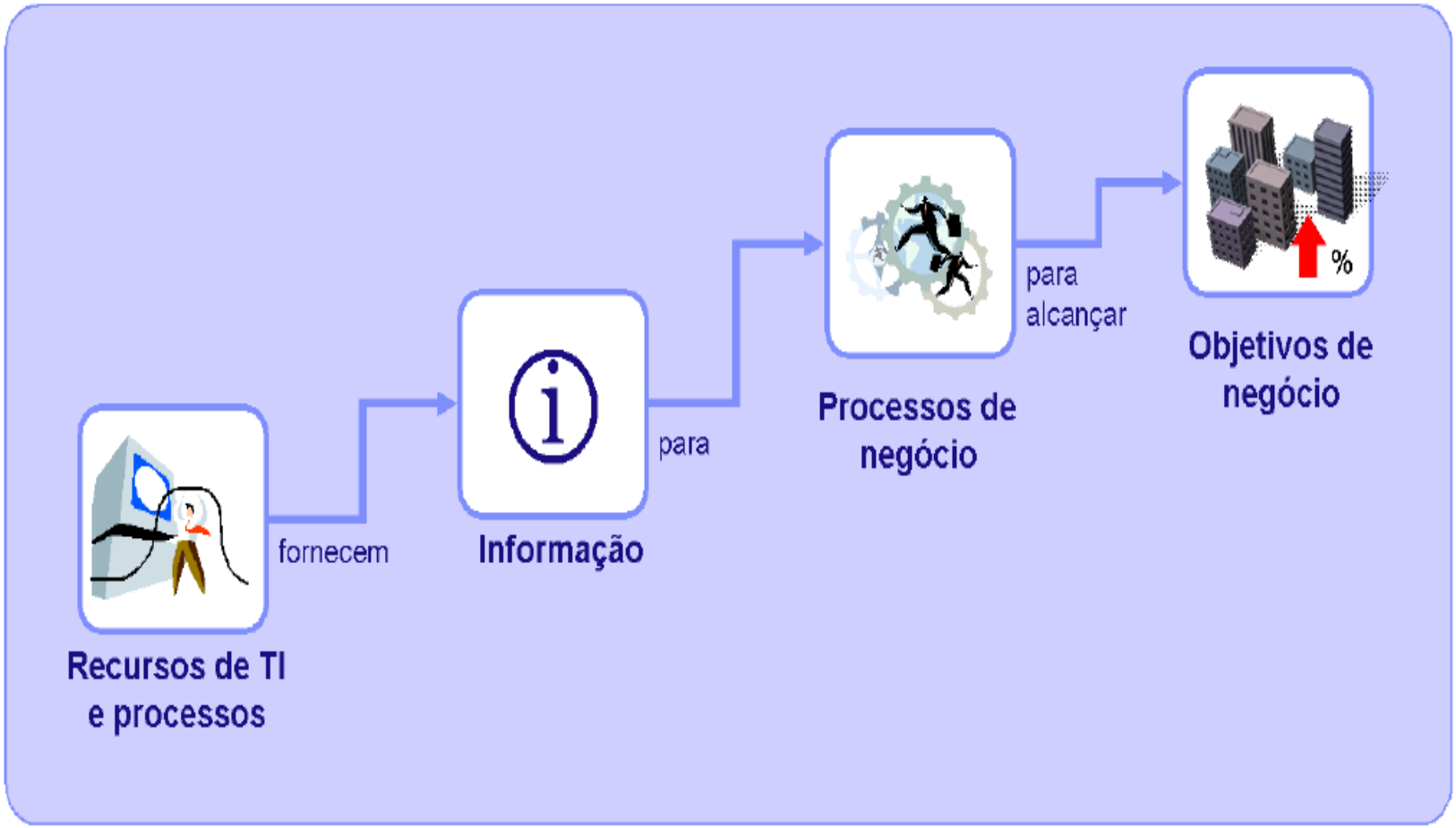
CUBO DO COBIT

COBIT - ÁREAS DE FOCO

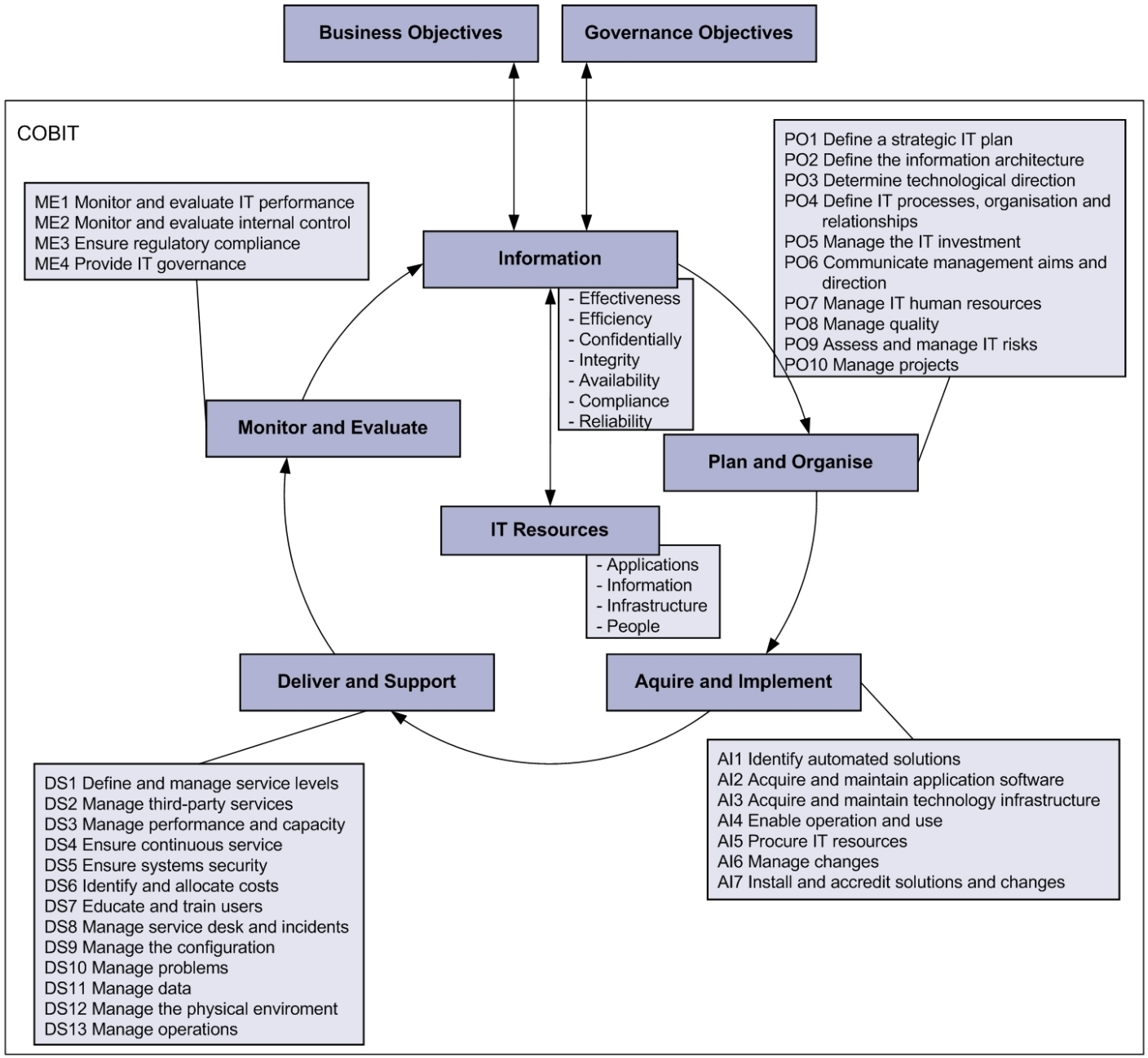
COBIT®
GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY

DOWNLOAD GUIA COBIT 4.1 FREE

COBIT



Fonte: adaptado do ITGI, COBIT 4.1



PO1 Define a Strategic IT Plan

From	Inputs
PO5	Cost-benefits reports
PO9	Risk assessment
PO10	Updated IT project portfolio
DS1	New/updated service requirements; updated IT service portfolio
*	Business strategy and priorities
*	Programme portfolio
ME1	Performance input to IT planning
ME4	Report on IT governance status; enterprise strategic direction for IT

* Inputs from outside COBIT

Outputs	To						
Strategic IT plan	PO2...PO6		PO8	PO9	AI1	DS1	
Tactical IT plans	PO2...PO6		PO9	AI1	DS1		
IT project portfolio	PO5	PO6	PO10	AI6			
IT service portfolio	PO5	PO6	PO9	DS1			
IT sourcing strategy	DS2						
IT acquisition strategy	AI5						

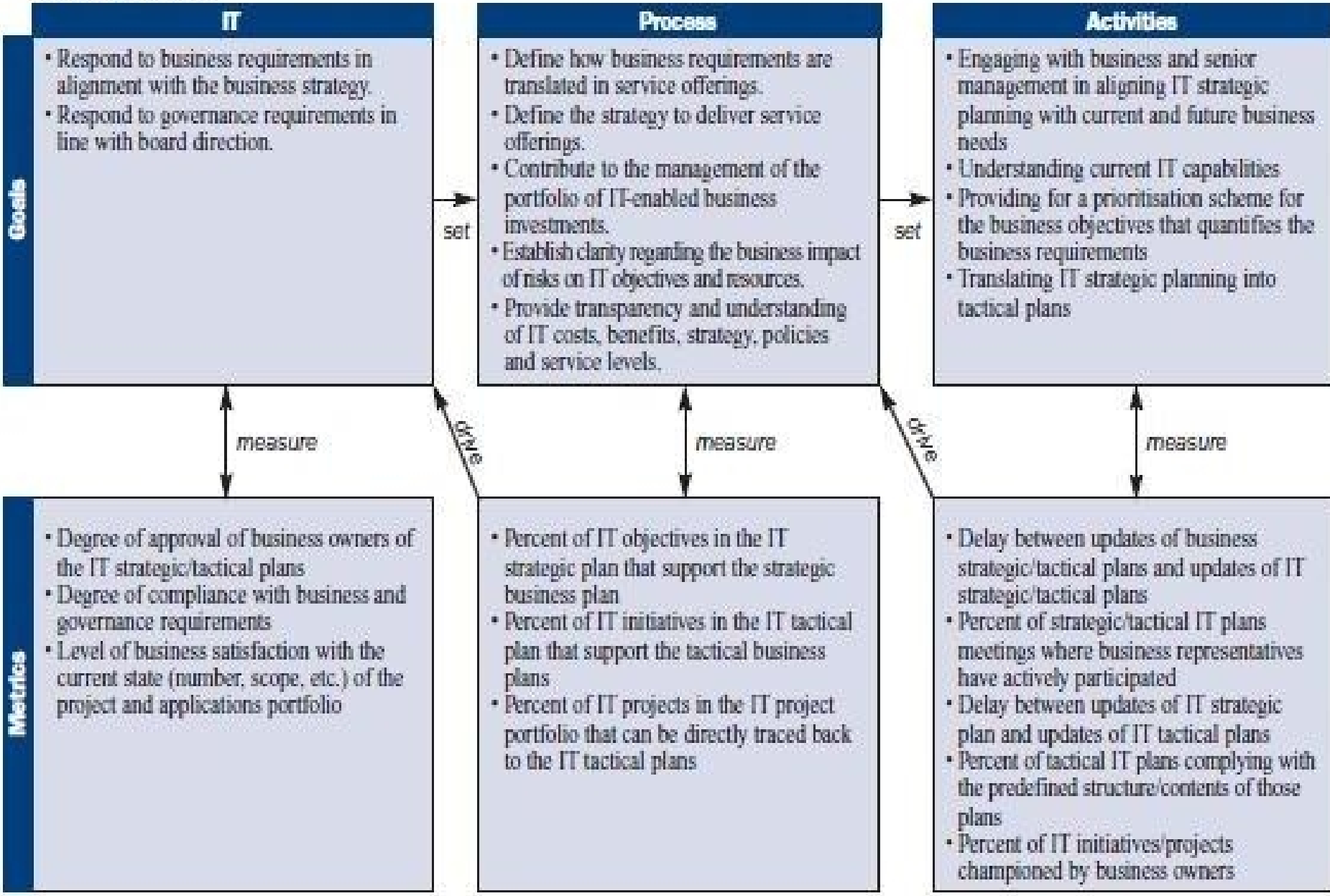
RACI Chart

Functions

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Link business goals to IT goals.	C	I	A/R	R	C						
Identify critical dependencies and current performance.	C	C	R	A/R	C	C	C	C	C		C
Build an IT strategic plan.	A	C	C	R	I	C	C	C	C	I	C
Build IT tactical plans.	C	I		A	C	C	C	C	C	R	I
Analyse programme portfolios and manage project and service portfolios.	C	I	I	A	R	R	C	R	C	C	I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



Modelo de processos do COBIT (34 processos)

ME1 Monitorar e avaliar o desempenho da TI
ME2 Monitorar e avaliar os controles internos
ME3 Assegurar conformidade regulatória
ME4 Fornecer Governança de TI

PO1 Definir um plano estratégico de TI
PO2 Definir a arquitetura de informação
PO3 Determinar o direcionamento tecnológico
PO4 Definir processos de TI, a organização e relacionamentos
PO5 Gerenciar o investimento em TI
PO6 Comunicar metas e diretivas gerenciais
PO7 Gerenciar os recursos humanos
PO8 Gerenciar a qualidade
PO9 Avaliar e gerenciar riscos de TI
PO10 Gerenciar projetos

DS1 Definir e gerenciar níveis de serviços
DS2 Gerenciar serviços de terceiros
DS3 Gerenciar o desempenho e capacidade
DS4 Garantir a continuidade dos serviços
DS5 Garantir a segurança dos sistemas
DS6 Identificar e alocar custos
DS7 Educar e treinar usuários
DS8 Gerenciar central de serviços e incidentes
DS9 Gerenciar a configuração
DS10 Gerenciar os problemas
DS11 Gerenciar os dados
DS12 Gerenciar o ambiente físico
DS13 Gerenciar as operações

Fonte: Adaptado do ITGI, COBIT 4.1

AI1 Identificar as soluções automatizadas
AI2 Adquirir e manter software aplicativo
AI3 Adquirir e manter infraestrutura de tecnologia
AI4 Permitir operação e uso
AI5 Adquirir recursos de TI
AI6 Gerenciar mudanças
AI7 Instalar e validar soluções e mudanças

COBIT

Requisitos de qualidade	Qualidade (cumprimento de requisitos de SLA) Entrega (entregar a tempo) Custo (dentro do orçamento esperado)
Requisitos Fiduciários (COSO)	Eficácia e eficiência operacional Confiabilidade dos relatórios financeiros Cumprimento de leis e regulamentos
Requisitos de segurança	Confidencialidade Integridade Disponibilidade

VANTAGENS DA IMPLEMENTAÇÃO COBIT

- Mapeamento dos objetivos de TI com os objetivos do negócio e *vice-versa*
- Compartilhamento e entendimento de todas as partes interessadas, baseado em uma linguagem comum
- Alinhamento, baseado no foco em negócio
- Uma visão de que o que TI faz é compreendida pela Gerência
- Geralmente aceito por terceiros e órgãos reguladores

Base Normativa para Atuação na área de Tecnologia da Informação

- INSTRUÇÃO NORMATIVA Nº 4 (19/05/2008)

Dispõe sobre o processo de contratação de serviços de TI pela Administração Pública Federal direta, autárquica e fundacional. A norma contempla as fases de planejamento de contratação, seleção do fornecedor e gerenciamento do contrato.

-DECRETO 3.505/2000

Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

Base Normativa para Atuação na área de TI
Acórdãos TCU

CONTRATAÇÃO DE SERVIÇOS OU OBRAS PELA ADMINISTRAÇÃO PÚBLICA FEDERAL

Acórdão nº 1.558/2003-TCU-Plenário, item 9.3.11: "(...) ao proceder a **licitação de bens e serviços de informática**, elabore previamente minucioso planejamento, realizado em harmonia com o **planejamento estratégico da unidade e com o seu plano diretor de informática** (...)";

Acórdão nº 2.094/2004-TCU-Plenário, item 9.1.1: "(...) todas as aquisições devem ser realizadas em harmonia com o **planejamento estratégico da instituição** (...)"

Base Normativa para Atuação na área de TI - Acórdãos TCU

Acórdão 1603/2008 - Plenário

"9.1.1. promovam ações com o objetivo de disseminar a importância do **planejamento estratégico**, procedendo, inclusive mediante orientação normativa, ações voltadas à implantação e/ou aperfeiçoamento de **planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI**"

Acórdão 1603/2008 - Plenário

"9.1.2. atentem para a necessidade de dotar **a estrutura de pessoal de TI do quantitativo de servidores efetivos** necessário ao pleno desempenho das atribuições do setor"

Base Normativa para Atuação na área de TI - Acórdãos TCU

Acórdão 1603/2008 - Plenário

"9.1.3. orientem sobre a importância do **gerenciamento da segurança da informação**, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a **gestão da continuidade do negócio**"

Acórdão 1603/2008 - Plenário

"9.1.4. estimulem a adoção de **metodologia de desenvolvimento de sistemas**, procurando assegurar, nesse sentido, níveis razoáveis de padronização e bom grau de confiabilidade e segurança"

Base Normativa para Atuação na área de TI - Acórdãos TCU

Acórdão 1603/2008 - Plenário

9.1.6. envidem esforços visando à implementação de **processo de trabalho formalizado de contratação de bens e serviços** de TI, bem como de gestão de contratos de TI"

Acórdão 1603/2008 - Plenário

"9.1.5. promovam ações voltadas à implantação e/ou aperfeiçoamento de **gestão de níveis de serviço de TI**, de forma a garantir a qualidade dos serviços prestados internamente"

Base Normativa para Atuação na área de TI - Acórdãos TCU

Acórdão no 1.999/2007-TCU- Plenário

"item 9.4.1.1 Os serviços de Tecnologia da Informação devem priorizar a contratação, **mensuração** e pagamento **por resultados**, razão pela qual apresentam-se mais específicos e complexos em termos de definição de especificações, modelagem, planejamento das necessidades, critérios e condições para realização de licitação e acompanhamento contratual.

Acórdão 1603/2008 - Plenário

9.1.8. introduzam **práticas voltadas à realização de Auditorias de TI**, que permitam a avaliação regular da conformidade, da qualidade, da eficácia e da efetividade dos serviços prestados.

Levantamento do Cenário de Governança de TI

- **Censo em todas as entidades do sistema S com base no levantamento dos seguintes pontos:**

- **Plano Diretor de TI**

- **Plano de segurança de TI**

- **Grau Informatização de processos estratégicos**

Levantamento do Cenário de Governança de TI

- Verificar o grau de comunicação entre os Departamentos Nacionais e Regionais com foco em uma Política Institucional de TI.

- Analisar atipicidades no Planejamento dos Sistemas de Informação (multiplicidades\ ausências).

- Verificar a atuação das áreas responsáveis pela TI segurança da informação, planejamento estratégico e gerenciamento de serviços de TI.

Conclusão

“Se a administração não tiver uma boa governança de tecnologia da informação terá seu funcionamento comprometido, gerando poucos ou nenhum benefício para a sociedade.” (Ministro-Substituto Augusto Sherman Cavalcanti, Junho/2007).

Obrigado !

Controladoria Geral da União

Secretaria Federal de Controle Interno

Visite o site:

www.cgu.gov.br