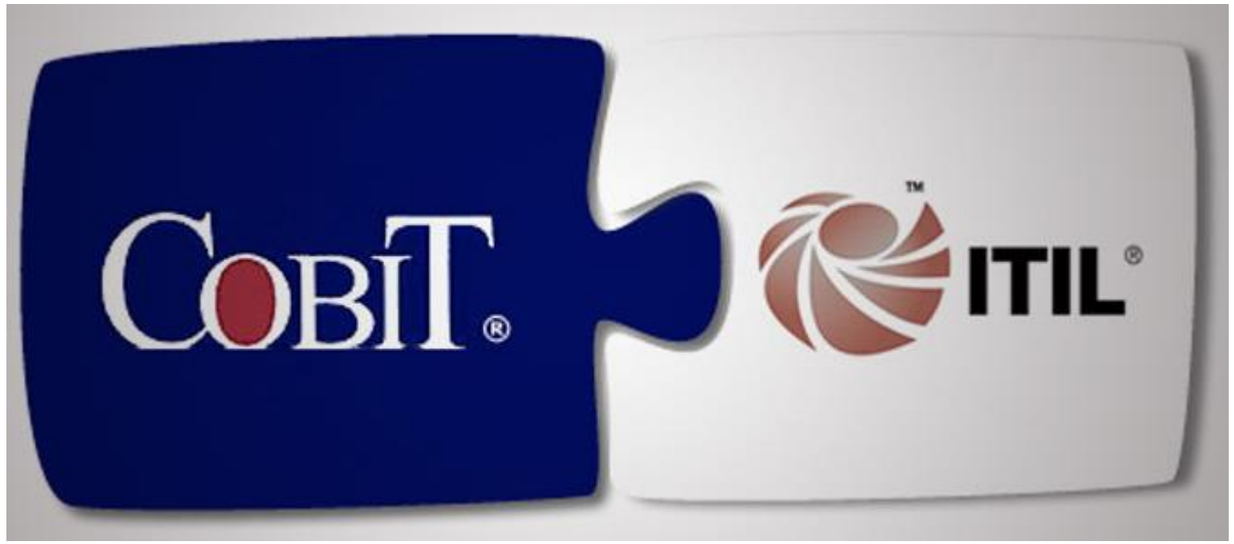
GESTÃO DE SERVIÇOS PARA TI

COBIT® 5

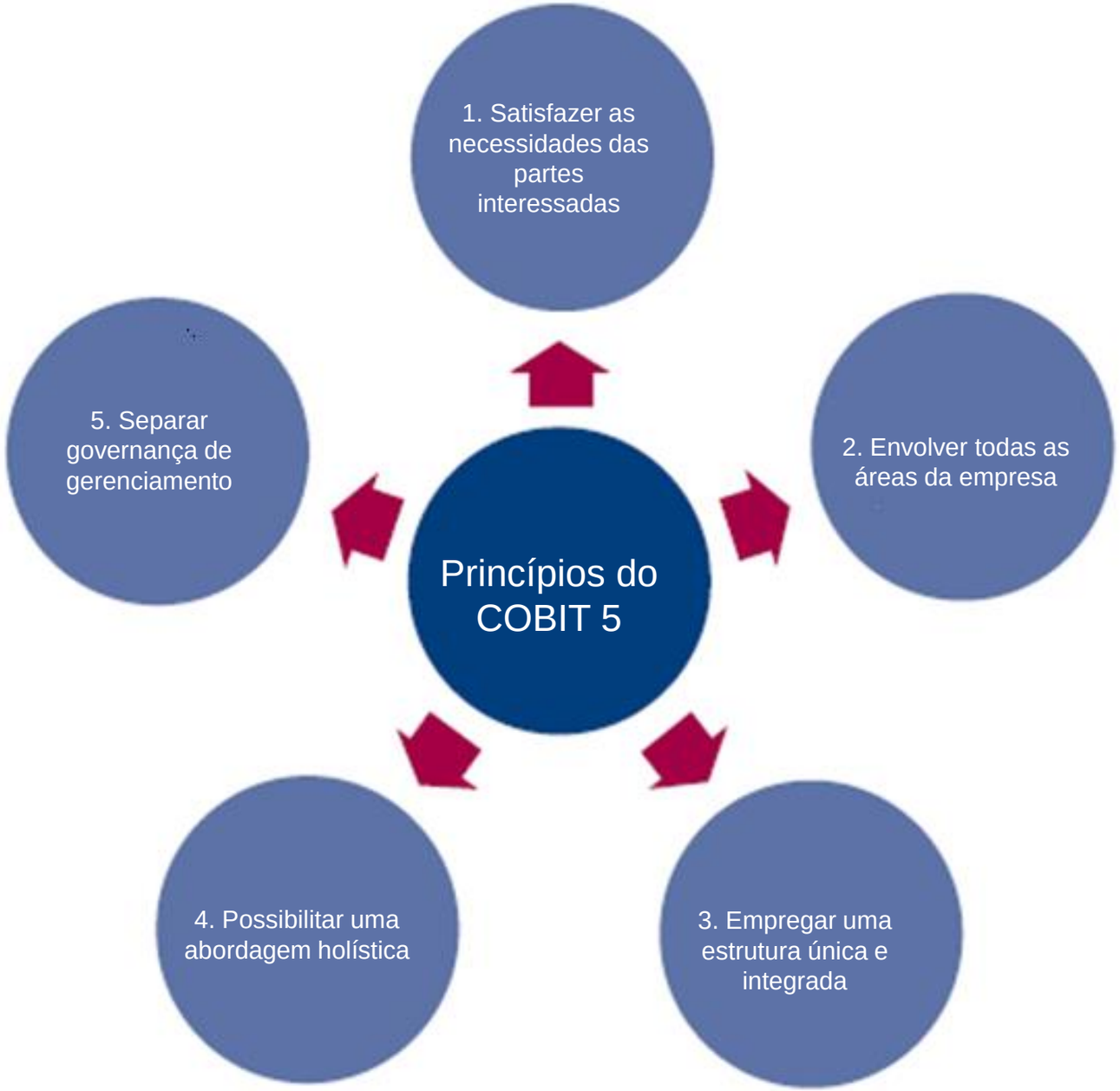
AN ISACA® FRAMEWORK

COBIT

- O **CobiT** é um conjunto de diretrizes baseadas em auditoria para processos, práticas e controles de TI, voltado para redução de risco, enfoca integridade, confiabilidade e segurança.
- Resumindo, o **CobiT** nada mais é do que um conjunto de ferramentas para a excelência em TI.

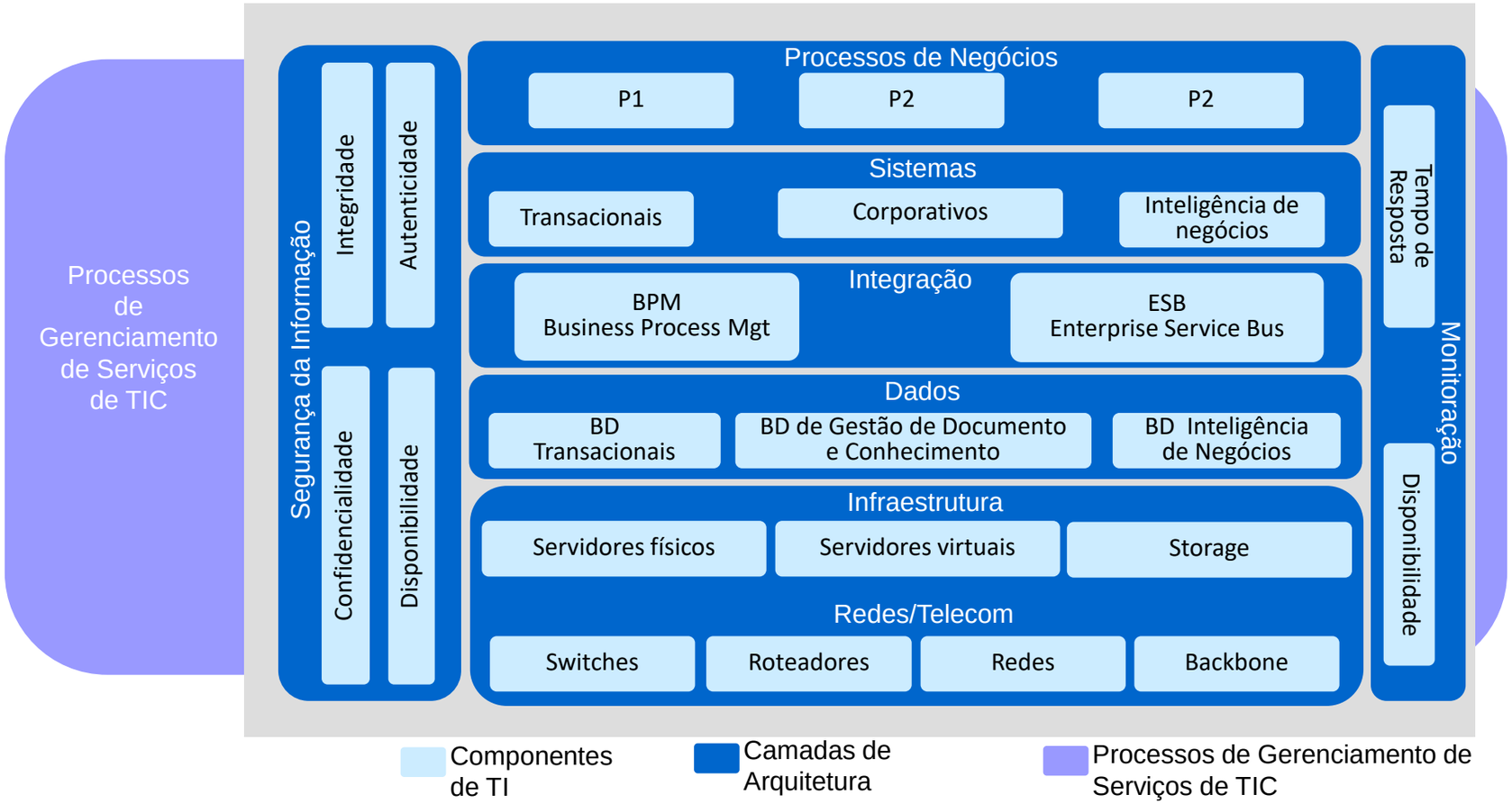


Princípios do Cobit



E qual melhor ferramenta pra Atender à Metodologia de auditoria?

TODAS AS CAMADAS E COMPONENTES DE TI SÃO OPERACIONADOS POR PROCESSOS QUE TRATAM DE TEMAS DE ESTRATÉGIA, PLANEJAMENTO, EXECUÇÃO, OPERAÇÃO E MEDIÇÃO DE DESEMPENHO DOS SERVIÇOS DE TI QUE APOIAM O NEGÓCIO.

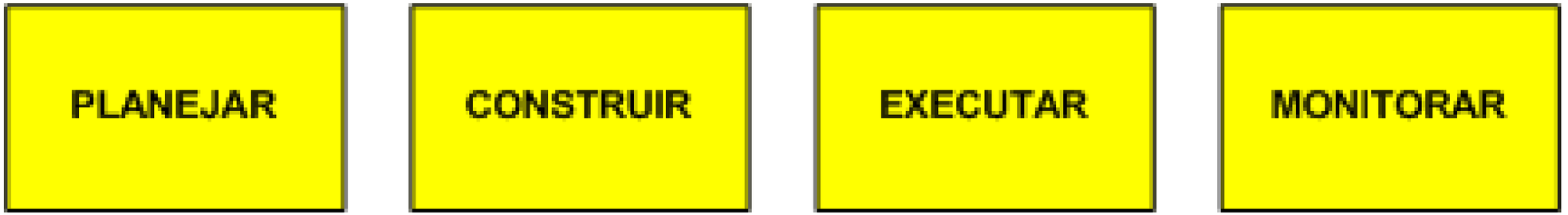


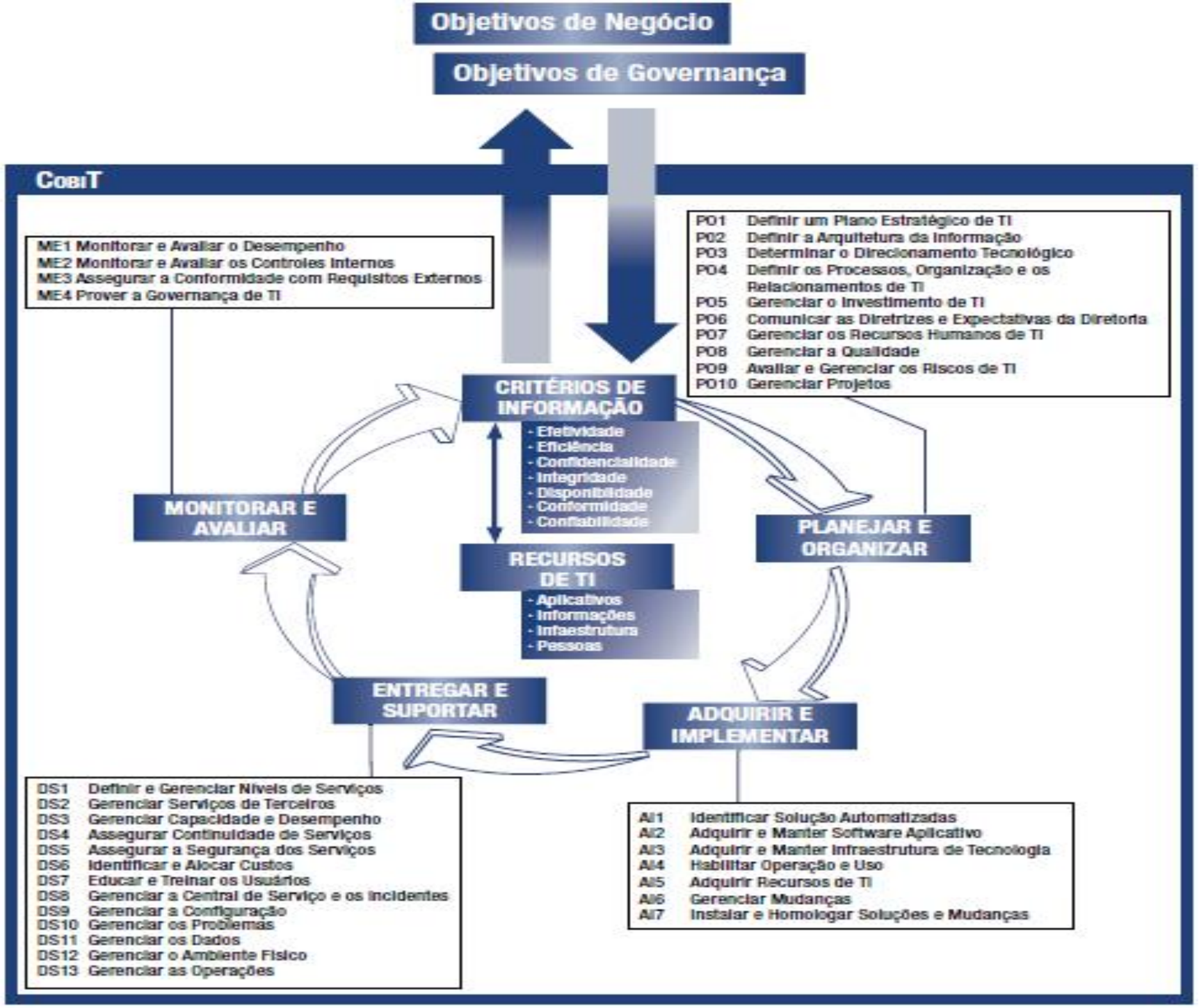
O **Enterprise Service Bus** (**ESB**) se refere à arquitetura de construção de software tipicamente implementado em tecnologias encontradas na categoria de produtos de infraestrutura híbrida.

COBIT

- O CobiT é focado em processos de TI possuindo a seguinte estrutura:

- O CobiT é utilizado pelas áreas de TI responsáveis por:

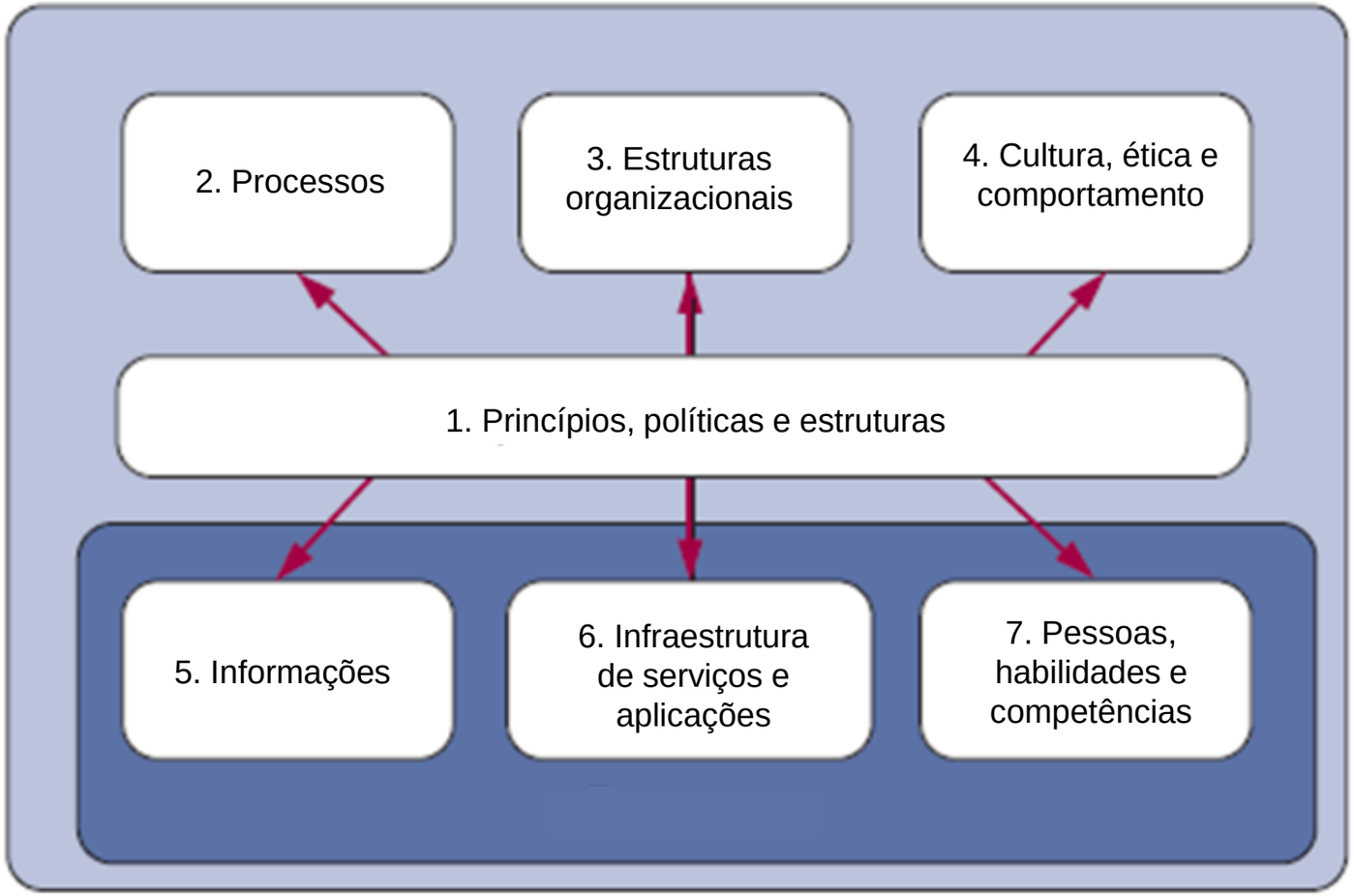



Objetivos de Negócio
Objetivos de Governança
CobiT
ME1 Monitorar e Avaliar o Desempenho
ME2 Monitorar e Avaliar os Controles Internos
ME3 Assegurar a Conformidade com Requisitos Externos
ME4 Prover a Governança de TI
PO1 Definir um Plano Estratégico de TI
PO2 Definir a Arquitetura da Informação
PO3 Determinar o Direcionamento Tecnológico
PO4 Definir os Processos, Organização e os Relacionamentos de TI
PO5 Gerenciar o Investimento de TI
PO6 Comunicar as Diretrizes e Expectativas da Diretoria
PO7 Gerenciar os Recursos Humanos de TI
PO8 Gerenciar a Qualidade
PO9 Avaliar e Gerenciar os Riscos de TI
PO10 Gerenciar Projetos
CRITÉRIOS DE INFORMAÇÃO
- Efetividade
- Eficiência
- Confidencialidade
- Integridade
- Disponibilidade
- Conformidade
- Confiabilidade
MONITORAR E AVALIAR
PLANEJAR E ORGANIZAR
RECURSOS DE TI
- Aplicativos
- Informações
- Infraestrutura
- Pessoas
ENTREGAR E SUPORTAR
ADQUIRIR E IMPLEMENTAR
DS1 Definir e Gerenciar Níveis de Serviços
DS2 Gerenciar Serviços de Terceiros
DS3 Gerenciar Capacidade e Desempenho
DS4 Assegurar Continuidade de Serviços
DS5 Assegurar a Segurança dos Serviços
DS6 Identificar e Alocar Custos
DS7 Educar e Treinar os Usuários
DS8 Gerenciar a Central de Serviço e os Incidentes
DS9 Gerenciar a Configuração
DS10 Gerenciar os Problemas
DS11 Gerenciar os Dados
DS12 Gerenciar o Ambiente Físico
DS13 Gerenciar as Operações
AI1 Identificar Solução Automatizadas
AI2 Adquirir e Manter Software Aplicativo
AI3 Adquirir e Manter Infraestrutura de Tecnologia
AI4 Habilitar Operação e Uso
AI5 Adquirir Recursos de TI
AI6 Gerenciar Mudanças
AI7 Instalar e Homologar Soluções e Mudanças

Estrutura do Cobit 5

- A estrutura do COBIT 5 ajuda as organizações a criarem o melhor valor possível com o uso de TI, mantendo o equilíbrio entre a realização dos benefícios e a otimização dos níveis de risco e do emprego de recursos.
- O COBIT 5 permite que a informação e tecnologias relacionadas sejam governadas e geridas de maneira holística em toda a empresa, envolvendo completamente todas as áreas da organização, de acordo com os interesses relativos à TI das partes interessadas internas e externas.
- Os **princípios** e **habilitadores** do COBIT 5 são gerais e úteis às organizações de qualquer porte, sejam elas comerciais, sem fins lucrativos ou do setor público.

HABILITADORES DO COBIT 5

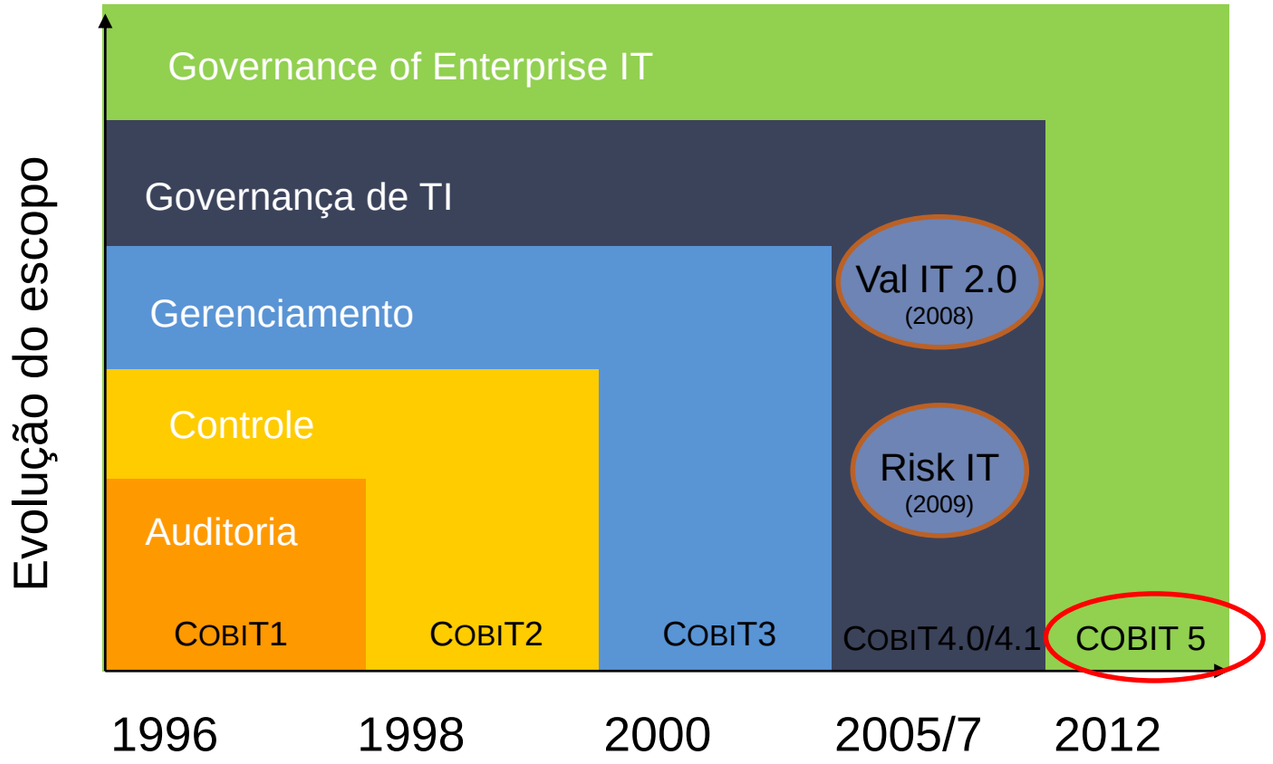


Fonte: COBIT® 5, figura 12. © 2012 ISACA® Todos os direitos reservados.

Governança e Gerenciamento

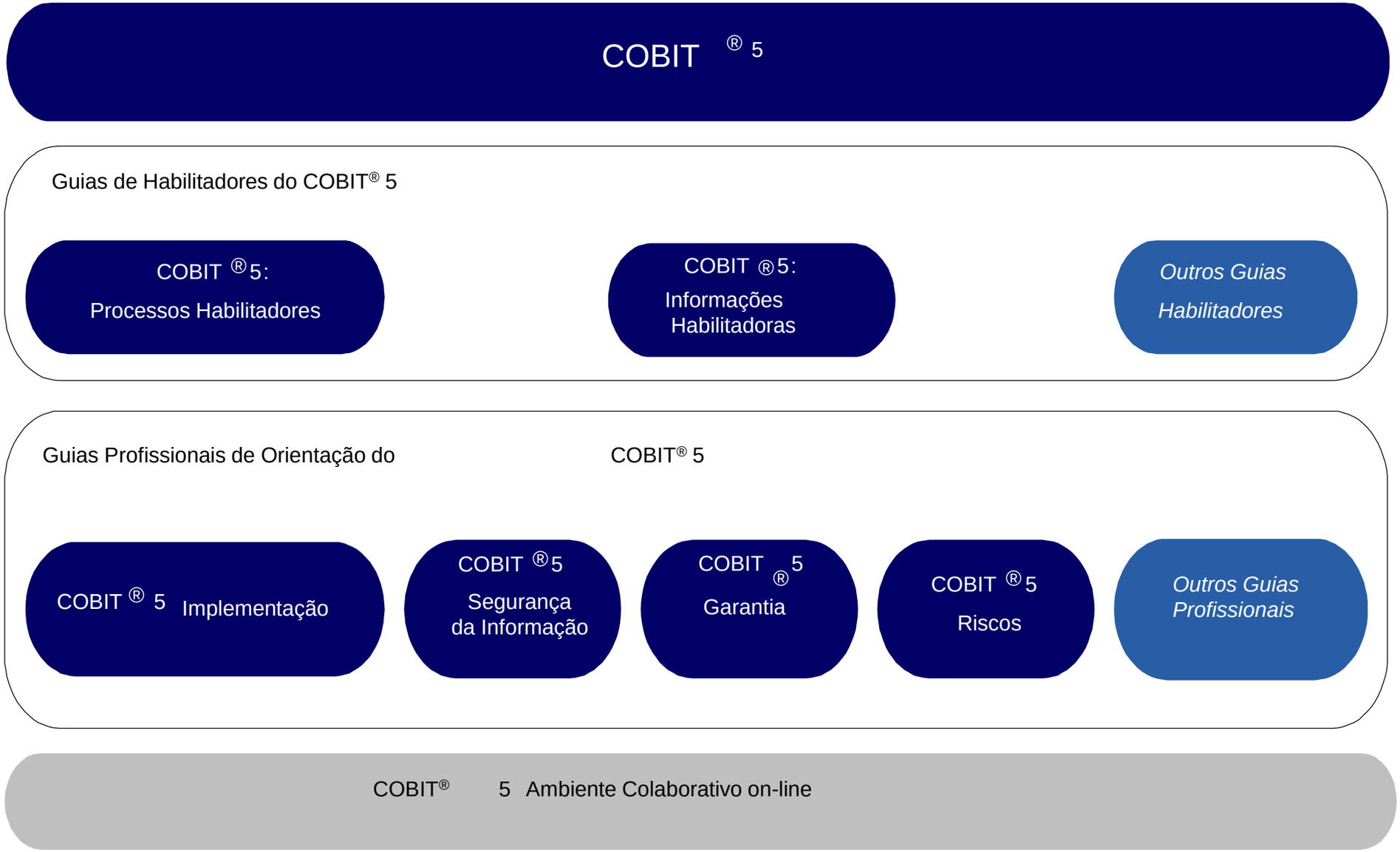
- A Governança garante que todos os objetivos da organização sejam alcançados por meio da avaliação das necessidades, condições e opções das partes interessadas, da definição de diretrizes, com gestão de prioridades e tomada de decisões, e do monitoramento do desempenho, da conformidade e da evolução dos processos em comparação com as diretrizes e os objetivos acordados.
- O gerenciamento planeja, desenvolve, executa e monitora as atividades de acordo com as diretrizes definidas pelo órgão de governança para alcançar os objetivos da empresa.

COBIT 5: UMA ESTRUTURA EMPRESARIAL VOLTADA PARA O NEGÓCIO



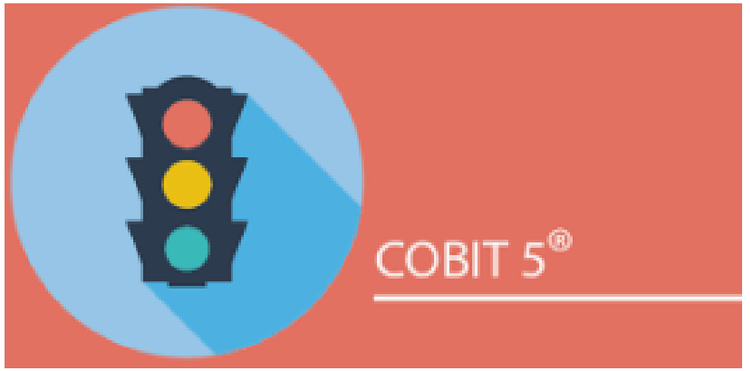
Estrutura empresarial da ISACA, extraída do site www.isaca.org/cobit

Família de Produtos COBIT



5 Princípios do Cobit 5

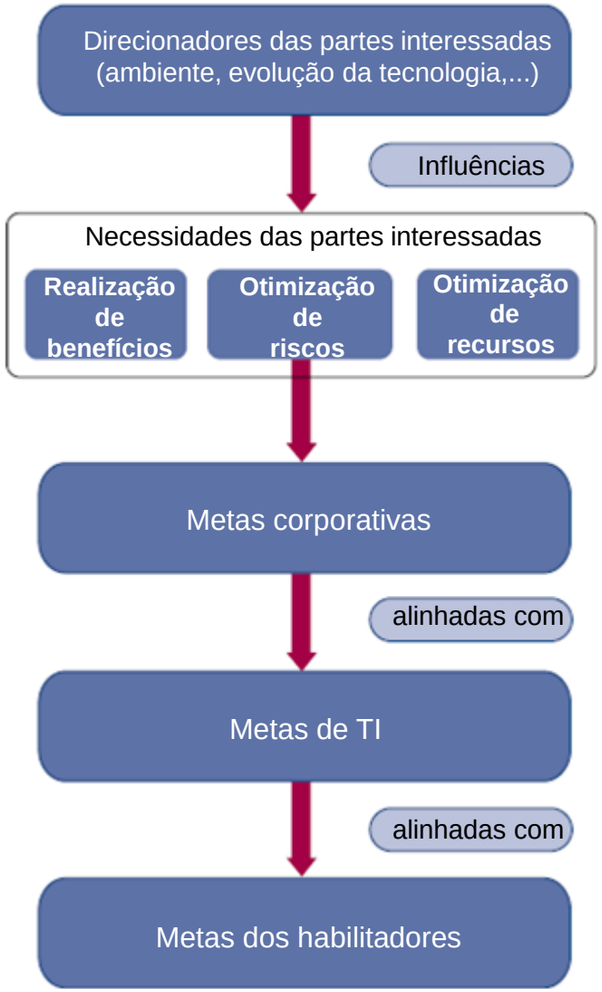
1. Satisfazer as necessidades das partes interessadas
2. Envolver todas as áreas da empresa
3. Empregar uma estrutura única e integrada
4. Possibilitar uma abordagem holística
5. Separar governança de gerenciamento



Satisfazer as necessidades das partes interessadas

- As organizações existem para criar valor para suas partes interessadas.

Fonte: COBIT® 5, figura 3. © 2012 ISACA® Todos os direitos reservados.



Fonte: COBIT® 5, figura 4. © 2012 ISACA®
Todos os direitos reservados.

Envolver todas as áreas da empresa

- O COBIT 5 aborda a governança e o gerenciamento da informação e tecnologias relacionadas sob uma perspectiva ampla, que envolve toda a organização.
- Isso significa que o COBIT 5:
  - Integra a governança corporativa de TI com a governança empresarial, ou seja, o sistema de governança de TI proposto pelo COBIT 5 se integra perfeitamente com qualquer sistema de governança porque o COBIT 5 está alinhado com as visões de governança mais recentes.
  - Abrange todas as funções e todos os processos da empresa; o COBIT 5 não foca somente as 'funções de TI', mas trata a informação e as tecnologias relacionadas como ativos com os quais todos da empresa devem lidar, como qualquer outro ativo da empresa.

Empregar uma estrutura única e integrada

- O COBIT 5 está alinhado com as estruturas e os padrões mais recentes e relevantes utilizados nas empresas:
  - Corporativos: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000
  - Relacionados à TI: ISO/IEC 38500, ITIL, série ISO/IEC 27000, TOGAF, PMBOK/PRINCE2, CMMI
  - Etc.
- Isso permite à empresa utilizar o COBIT 5 como um integrador global das estruturas de governança e gerenciamento.
- A ISACA planeja oferecer aos usuários do COBIT o recurso de mapeamento das práticas e atividades de referências de terceiros.

Habilitadores do COBIT 5

- Fatores que, individual e coletivamente, influenciam o funcionamento dos processos — no caso do COBIT, a governança e o gerenciamento corporativos da TI.
- Impulsionados pela cascata de metas, ou seja, os objetivos de alto nível relacionados a TI definem quais resultados os diferentes habilitadores devem alcançar.
- Descritos pela estrutura do COBIT 5 em sete categorias.

Governança x Gerenciamento

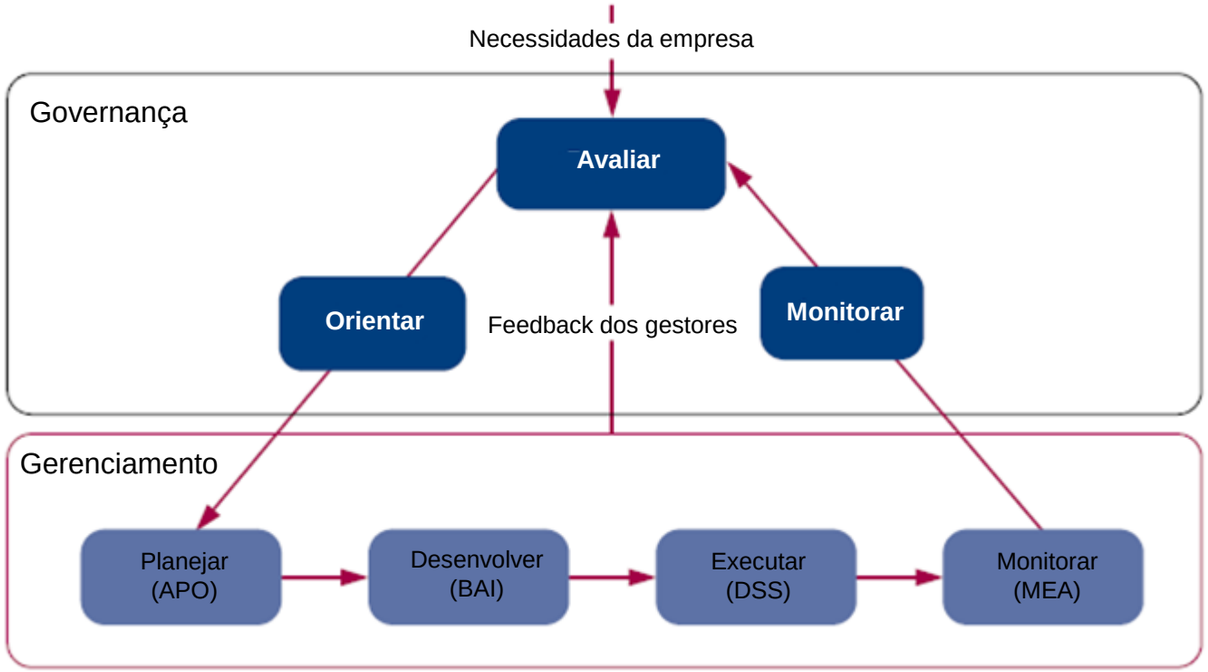
- A estrutura do COBIT 5 faz uma distinção clara entre governança e gerenciamento.
- Essas duas disciplinas:
  - Englobam tipos diferentes de atividades
  - Demandam estruturas organizacionais diferentes
  - Têm finalidades diferentes
- Governança - Na maioria das organizações, governança é responsabilidade do conselho de administração, sob a liderança do presidente.
- Gerenciamento - Na maioria das organizações, o gerenciamento é responsabilidade dos executivos, sob a liderança do CEO.

Governança x Gerenciamento

- A governança garante que as necessidades, condições e opções das partes interessadas sejam avaliadas para a definição de objetivos corporativos equilibrados e consensuais a serem alcançados por meio da definição de diretrizes, com gestão de prioridades e tomada de decisões, e do monitoramento do desempenho e da conformidade em comparação com as diretrizes e os objetivos acordados.
- O gerenciamento planeja, desenvolve, executa e monitora as atividades de acordo com as diretrizes definidas pelo órgão de governança para alcançar os objetivos da empresa.

Governança x Gerenciamento

- O COBIT 5 não é prescritivo, mas defende que as organizações implementem os processos de governança e gerenciamento, contemplando as principais áreas, conforme ilustração a seguir.



Fonte: COBIT® 5, figura 15. © 2012 ISACA® Todos os direitos reservados.

Organização do trabalho da auditoria
Planejamento

- 1º Passo
  - Conhecer o ambiente a ser auditado: Levantamento dos dados acerca do ambiente computacional (fluxo de processamento, recursos humanos e materiais envolvidos, arquivos processados, relatórios e telas produzidos).
- 2º Passo:
  - Determinar os pontos de controle (processos críticos)
- 3º Passo: Definição dos objetivos da auditoria:
  - Técnicas a serem aplicadas
  - Prazos de execução
  - Custos de execução
  - Nível de tecnologia a ser utilizada

Organização do trabalho da auditoria
Planejamento

- 4º Passo:
  - Estabelecimento de critérios para análise de risco
- 5o. Passo:
  - Análise de Risco
  - Avaliar para cada ponto de controle o grau de risco apresentado para posterior hierarquização:
  - Grau de Risco
    - 1 – Muito Fraco
    - 2 – Fraco
    - 3 – Regular
    - 4 – Forte
    - 5 – Muito forte
- 6º Passo:
  - Hierarquização dos pontos de controle

Organização do trabalho da auditoria
Execução

- 1o. passo: Escolher a equipe.
  - Perfil e histórico profissional
  - Experiência na atividade
  - Conhecimentos específicos
  - Formação acadêmica
  - Línguas estrangeiras
  - Disponibilidade para viagens, etc.

Organização do trabalho da auditoria
Execução

- 2o. passo: Programar a equipe
  - Gerar programas de trabalho
  - Selecionar procedimentos apropriados
  - Incluir novos procedimentos
  - Classificar trabalhos por visita
  - Orçar tempo e registrar o real

- 3o. passo: Execução dos trabalhos
  - Dividir as tarefas de acordo com a formação, experiência e treinamento dos auditores
  - Efetuar supervisão para garantir a qualidade do trabalho e certificar que as tarefas foram feitas corretamente

Organização do trabalho da auditoria
Execução

- 4o. passo: Revisão dos papéis
  - Verificar pendências e rever o papel de cada auditor para suprir as falhas encontradas

- 5o. passo: Avaliação da equipe
  - Avaliar o desempenho, elogiando os pontos fortes e auxiliando no reconhecimento e superação de fraquezas do auditor
  - Ter um sistema de avaliação de desempenho automatizado

Organização do trabalho da auditoria
Documentação do trabalho

- Documentação de todo o processo de Auditoria de Sistemas executado.

Artefatos gerados pela Auditoria de sistemas

- Relatório de fraquezas de controle interno
- Certificado de controle interno
- Relatório de redução de custos
- Manual de auditoria do ambiente
- Pastas contendo a documentação obtida pela Auditoria de Sistemas

Relatório de Fraquezas de controle interno

- Objetivo do projeto de auditoria
- Pontos de controle auditados
- Conclusão alcançada a cada ponto de controle
- Alternativas de solução propostas

Certificado de Controle Interno

- Indica se o ambiente está em boa, razoável ou má condição em relação aos parâmetros de controle interno. Apresenta a opinião da auditoria em termos globais e sintéticos.

Relatório de redução de custos

- Tem por objetivo explicitar as economias financeiras a serem feitas com a adoção das recomendações efetuadas. Serve de base para a realização das análises de retorno de investimento e do custo/beneficio da auditoria de auditoria de sistemas.

Manual da auditoria do ambiente auditado

- Armazena o planejamento da auditoria, os pontos de controle testados e serve como referência para futuras auditorias.

Pastas contendo a documentação da auditoria de sistemas

- Irá conter toda a documentação do ambiente e dos trabalhos realizados como: relação de programas, relação de arquivos do sistema, relação de relatórios e telas, fluxos, atas de reunião, etc.

Apresentação dos resultados da auditoria à alta administração

- Objetividade na transmissão dos resultados
- Esclarecimento das discussões realizadas entre a auditoria e os auditados
- Clareza nas recomendações das alternativas de solução
- Coerência da atuação da Auditoria
- Apresentação da documentação gerada
- Explicação do conteúdo de cada documento.

Benefícios para a organização

- Manter informações de qualidade para subsidiar as decisões.
- Gerar valor dos investimentos habilitados por TI, ou seja, atingir metas estratégicas e realizar os benefícios por meio do uso eficaz e inovador de TI.
- Alcançar excelência operacional com a aplicação confiável e eficiente da tecnologia.
- Manter os riscos relacionados à TI em um nível aceitável.
- Otimizar os custos de serviços e tecnologias de TI.

Entrega de Valor às Partes Interessadas

- Entregar valor às partes interessadas requer **governança e gerenciamento** dos ativos de informação e tecnologia (TI).
- As diretorias, os executivos e gestores das organizações precisam **tratar a TI** como qualquer outra parte importante da organização.
- Os requisitos externos de **conformidade legal, regulatória e contratual** relativos ao uso de informação e tecnologia pelas organizações estão aumentando, ameaçando o valor caso não sejam cumpridos.
- **O COBIT 5 se propõe a oferecer uma estrutura abrangente (boas práticas) que ajuda as organizações a atingirem suas metas e entregarem valor com estratégias eficazes de governança e gerenciamento de TI.**

Abordagem Holística Cobit 5

1. Processos - descrevem um conjunto organizado de práticas e atividades para atingir certos objetivos e produzir um conjunto de resultados que auxiliem no cumprimento das metas gerais relacionadas à TI
2. Estruturas organizacionais - são as principais entidades responsáveis pela tomada de decisões em uma organização
3. Cultura, ética e comportamento - dos indivíduos e da organização, muito frequentemente são subestimados como fatores de sucesso nas atividades de governança e gerenciamento
4. Princípios, políticas e estruturas - são veículos que traduzem o comportamento desejado em orientações práticas para a gestão cotidiana
5. Informação - está arraigada em toda a organização, ou seja, representa todas as informações produzidas e utilizadas na empresa. As informação são necessárias para manter a organização em funcionamento e bem governada, mas no nível operacional, a informação, com frequência, é o produto principal da empresa.
6. Serviços, infraestrutura e aplicações - incluem a infraestrutura, a tecnologia e as aplicações que fornecem à organização os serviços e o processamento de TI
7. Pessoas, habilidades e competências - estão relacionadas com pessoas e são necessárias à execução bem-sucedida das atividades e à tomada de decisões corretas e adoção de ações corretivas

BIBLIOGRAFIA

- IMONIANA, J. O. . Auditoria de sistemas de informação. 1. ed. São Paulo: Atlas, 2005. v. 1. 115.

- SILVA JÚNIOR, J. B ? Coordenador. Auditoria em ambiente de internet. 1. ed. São Paulo : Atlas, 2001. v. 1.

- TRIBUNAL DE CONTAS DA UNIÃO. Manual de Auditoria de Sistemas, 2008. Disponível em http://portal2.tcu.gov.br/tecnologia_informacao/sumarios