AAL | Consultoria & Auditoria

MOLDANDO NEGÓCIOS EM PROL DO SUCESSO

AGNALDO ALVES

Formação Acadêmica

Contador, pela UFPR.
Pós-Graduado em Controladoria, pela UFPR.
MBA em Auditoria, pela UFPR.

Experiência profissional

Auditor Interno e Externo em diversas empresas nacionais e multinacionais.
Diretor Adjunto, Conselheiro Fiscal.
Contador Perito Assistente Técnico em diversos processos da área: Cível.
Professor de Cursos de Graduação e Pós-Graduação Presencial e a Distância.
Palestrante.

ENDEREÇOS DE NOSSAS CREDENCIAIS

https://www.grupoaal.com.br

https://www.linkedin.com/in/agnaldo-alves-08b08086/

http://lattes.cnpq.br/1990536236046136;

AAL | Consultoria & Auditoria

A **AAL** é uma empresa de Consultoria, atuando nos segmentos industrial, comercial e prestação de serviços.

Tem como diferencial competitivo a especialização na Gestão Estratégica de Negócios, contribuindo com a Manutenção, Crescimento, Fortalecimento e Valorização da Imagem da Marca e Sustentabilidade das Empresas.

AAL | Consultoria & Auditoria

COSO
&
SOX

AAL | Consultoria & Auditoria

INTRODUÇÃO À LEI SARBANES-OXLEY (SOX)

A Lei Sarbanes-Oxley (Sarbanes-Oxley Act, normalmente abreviada em SOx ou Sarbox) é uma lei dos Estados Unidos criada em 30 de julho de 2002 por iniciativa do senador Paul Sarbanes (Democrata) e do deputado Michael Oxley (Republicano). Segundo a maioria dos analistas, esta lei representa a maior reforma do mercado de capitais americano desde a introdução de sua regulamentação, logo após a crise financeira de 1929.

Sen. Paul Sarbanes (D–MD) e o Rep. Michael G. Oxley (R–OH-4), os coautores da Sarbanes–Oxley Act (fonte: Wikipédia)

A criação desta lei foi uma consequência das fraudes e escândalos contábeis que, na época, atingiram grandes corporações nos Estados Unidos (Enron, Arthur Andersen, WorldCom, Xerox etc…), e teve como intuito tentar evitar a fuga dos investidores causada pela insegurança e perda de confiança em relação as escriturações contábeis e aos princípios de governança nas empresas.

A **SOX** se aplica a todas as empresas, sejam elas americanas ou estrangeiras, que tenham ações registradas na SEC (*Securities and Exchange Comission*, o equivalente americano da CVM brasileira). Isso inclui as empresas estrangeiras que possuem programas de ADRs *(American Depositary Receipts)*, do nível 2 ou 3, nas bolsas de valores dos EUA.

Conceito Sarbanes Oxley

A Lei *Sarbanes-Oxley* é uma reação da legislação americana aos escândalos financeiros da *Enron*, *WorldCom*, entre outros. Foi promulgada em janeiro de 2002, nos Estados Unidos.
Esta lei estabelece regras para Governança Corporativa relativas à divulgação e à emissão de relatórios financeiros.

O objetivo da Lei é:

- Coibir abusos, ampliando exigências de governança corporativa;
- Implementar mudanças efetivas e sustentáveis para recuperar a confiança dos investidores no mercado de capitais;
- Aumentar a transparência das informações geradas pelas empresas e instituições do mercado de capitais (os investidores preocupam-se com a forma como seus investimentos são gerenciados e como são protegidos)
- Desencorajar afirmações dos executivos de que "não tinham conhecimento" das atividades duvidosas praticadas por suas companhias, tais como:

- Participações não registradas nos livros,
- Reconhecimento de receitas impróprias,
- Outras falhas de controle interno.

Destina-se às empresas americanas, mas atinge as companhias de capital aberto com ações negociadas na Bolsa de Nova Iorque – NYSE.

Para atender o disposto na Lei *Sarbanes-Oxley*, a Companhia vem adotando medidas para ter maior confiança em seus controles internos. Contou com o apoio de consultoria externa da *Ernst & Young*, para auxiliar o corpo funcional a mapear e certificar todos os controles internos da Copel. A partir de 2006, estes controles serão testados pela Auditoria Externa Contratada da Copel, que deverá emitir um parecer sobre a confiabilidade de nossos sistemas e controles, que será incluído no teor do Relatório 20-F.

Dividida em onze títulos (capítulos), com um número variável de seções cada um, totalizando 69 seções (artigos), a **SOX** obriga as empresas a reestruturarem processos para aumentar os controles, a segurança e a transparência na condução dos negócios, na administração financeira, nas escriturações contábeis e na gestão e divulgação das informações. Na prática define por lei e rende obrigatórias uma série de medidas que já eram consideradas, no mundo todo, como práticas de boa governança corporativa.

A **SOX** prevê a criação, nas empresas, de mecanismos de auditoria e segurança confiáveis, definindo regras para a criação de comitês encarregados de supervisionar suas atividades e operações, formados em boa parte por membros independentes. Isso com o intuito explícito de evitar a ocorrência de fraudes e criar meios de identificá-las quando ocorrem, reduzindo os riscos nos negócios e garantindo a transparência na gestão.

A **SOX** torna os Diretores Executivos e Diretores Financeiros explicitamente responsáveis por estabelecer e monitorar a eficácia dos controles internos em relação aos relatórios financeiros e a divulgação de informações. As empresas de auditoria e os advogados contratados ganham maior independência, mas também aumenta muito o grau de responsabilidade sobre seus atos. Também aumenta muito a regulamentação sobre as modalidades de contratação de tais serviços (auditoria, legais etc…), sobre o relacionamento entre empresa e estes prestadores de serviços e sobre os limites de atuação (serviços que podem e não podem ser prestados) e a gestão de eventuais conflitos de interesses.

Para supervisionar os processos de auditoria das empresas sujeitas a SOx, foi criado o Public Company Accounting Oversight Board (PCAOB ou seja Conselho de Auditores de Companhias Abertas) que tem a missão de estabelecer as normas de auditoria, controle de qualidade, ética e independência em relação aos processos de inspeção e a emissão dos relatórios de auditoria. São previstas inspeções às empresas de auditoria para obrigá-las a cumprir as regras estabelecidas e estar sempre em consonância com a SEC. Os auditores de empresas sujeitas a SOx deverão registrar-se no PCAOB.

A SOx se refere de forma explícita aos GAAP (Generally Acetes Accounting Principles), na versão US GAAP, para a definição de quais sejam as normas e práticas contábeis a serem aplicadas. É em andamento, sob a coordenação da SEC, um processo oficial de adoção do padrão IFRS (International Financial Reporting Standards), de influência européia e administrado pelo IASB (International Accounting Standards Board), no lugar do US GAAP, que deverá se concluir até 2016. Outra legislação relevante e explicitamente mencionada na SOx é o Securities Exchange Act de 1934.

As penalidades pelo descumprimento da SOx, em relação a integridade e fidedignidade das demonstrações financeiras e a certificação de demonstrativos em desacordo com a lei, são uma multa de até USD 1.000.000 e/ou a reclusão por até 10 anos. Quando o descumprimento da lei for intencional (normalmente com finalidades fraudulentas) a multa aumenta para até USD 5.000.000 e a reclusão pode chegar a 20 anos.

Os principais artigos da SOx (divididos por categoria) são os seguintes:

PCAOB:

- *Artigo 101*: Cria o Public Company Accounting Oversight Board.
- *Artigo 102*: Trata da organização do PCAOB e de suas atribuições.
- *Artigo 103*: Define regras e padrões de auditoria, controle de qualidade e independência.
- *Artigo 104*: Determina que o PCAOB crie um programa permanente de inspeção nas empresas de auditoria registradas na SEC.
- *Artigo 109*: Define o financiamento e taxas de funcionamento do PCAOB.

Independência do auditor:

- *Artigo 201*: Define serviços que são proibidos para os auditores dentro das companhias que auditam.
- *Artigo 202*: Determina a necessidade da aprovação prévia do comitê de auditoria para qualquer outro serviço prestado pelos auditores independentes da companhia.
- *Artigo 203*: Determina a rotatividade a cada 5 anos do sócio responsável por cada cliente, em empresa de auditoria.
- *Artigo 204*: Cria regras para comunicação entre os auditores contratados e o comitê de auditoria da companhia.

Responsabilidades da empresa:

- *Artigo 301*: Define as funções atribuídas e nível de independência do comitê de auditoria em relação à direção da empresa.
- *Artigo 302*: Determina a responsabilidade dos diretores das empresas, que devem assinar os relatórios certificando que as demonstrações e outras informações financeiras incluídas no relatório do período, apresentam todos os fatos materiais e que não contém nenhuma declaração falsa ou que fatos materiais tenham sido omitidos. Também devem declarar que divulgaram todas e quaisquer deficiências significativas de controles, insuficiências materiais e atos de fraude ao seu Comitê de Auditoria.
- *Artigo 303*: Proíbe a conduta imprópria de auditor por influência fraudulenta, coação ou manipulação, não importando se intencional ou por negligência. Proíbe diretores e funcionários da empresa de tomar qualquer medida para influenciar os auditores.
- *Artigo 305*: Define as responsabilidades e penalidades a cargo dos diretores da empresa.
- *Artigo 307*: Cria regras de responsabilidade para advogados obrigando-os a relatar evidências de violação importante da companhia para a qual prestam serviços, devendo reportar-se ao comitê de auditoria, se não forem ouvidos pela diretoria.

Aprimoramento das divulgações financeiras:

- *Artigo 401*: Obriga a divulgação das informações trimestrais e anuais sobre todo fato material não relacionado com o balanço, patrimonial, tais como: transações, acordos, obrigações realizadas com entidades não consolidadas, contingências e outras. Também exige a divulgação de informações financeiras não relacionadas com as normas geralmente aceitas (de acordo com o GAAP).
- *Artigo 402*: Obriga a divulgação das principais transações envolvendo a diretoria e os principais acionistas da companhia. Nenhum diretor ou funcionário graduado de companhia aberta poderá receber, direta ou indiretamente, empréstimos em companhia aberta.
- *Artigo 404*: Determina uma avaliação anual dos controles e procedimentos internos para a emissão de relatórios financeiros. Além disso, o auditor independente deve emitir um relatório distinto que ateste a asserção da administração sobre a eficácia dos controles internos e dos procedimentos executados para a emissão dos relatórios financeiros.
- *Artigo 406*: Define o Código de ética para os administradores, alta gerência e gerência.
- *Artigo 409*: Obriga a divulgação imediata e atual de informações adicionais relativas a mudanças importantes na situação financeiras ou nas operações da companhia.

Responsabilidade por fraude corporativa ou criminal:

- *Artigo 802*: Define as penalidades criminais por alteração / destruição / falsificação de documentos a serem utilizados nas vistorias da SEC.
- *Artigo 806*: Cria os meios de proteção aos funcionários de empresas de capital aberto que denunciarem fraude na companhia em que trabalham.
- *Artigo 807*: Define as penalidades criminais por prejudicar acionistas minoritários de empresas de capital aberto com informações inverídicas.

Aumento das penalidades para crimes de colarinho branco:

- *Artigo 906*: Aumenta a responsabilidade da diretoria sobre as demonstrações financeiras e define as penalidades para as infrações.

O Portal de Auditoria/Escola de Auditoria, vem desde 2005, através de seus profissionais, propagando Auditoria Interna como ferramenta de gestão pelos países de língua portuguesa, transcendendo o território físico do Brasil, dessa forma disponibilizamos aos nossos usuários e clientes conteúdos diversos sobre o tema, assim como diversos cursos para capacitação e desenvolvimento profissional.

Fraudes Contábeis e Internas

Panorama das diretrizes COSO e COBIT

COSO é a abreviação por “Committee of Sponsoring Organizations of the Treadway Commission”, uma organização Norte Americana privada, fundada em 1985, que se dedica a desenvolver e estudar assuntos gerenciais e de governança empresarial com o intuito de fornecer linhas guia ou diretrizes para os executivos. As áreas de principal interesse do COSO são Governança Corporativa, Ética de Negócios, Controles Internos, Gestão de Riscos Corporativos, Fraudes e Relatórios Financeiros.

Em Setembro de 1992 o COSO publicou um relatório intitulado “Internal Control - Integrated Framework” (Controles Internos e Estrutura Integrada), ou ICIF. Em 2004 publicou um novo relatório intitulada “Enterprise Risk Management - Integrated Framework” (Gestão de Riscos Corporativos – Estrutura Integrada), ou ERMIF, que é considerado uma evolução das questões relativas aos controles internos, focado no mais amplo problema da gestão de riscos corporativos. O COSO publicou vários outros estudos e relatórios ao longo dos anos, todos relacionados a gestão de riscos, controles internos e prevenção de fraudes.

A SEC (Securities and Exchange Commission) dos EUA, sugere e recomenda que as empresas adotem a estrutura de processos de controle definidos pelo COSO (ICIF) para que possam adimplir as regras definidas pela SOx (Lei Sarbanes-Oxley). Além disso o ICIF e a estrutura COSO são um dos padrões mais usados pelas companhias Norte Americanas para avaliar a própria observância as regras do FCPA.

A clássica estrutura do COSO, descrita no ICIF, é baseada em alguns conceito de base:

- Os Controles Internos são um processo. Se trata de um instrumento para uma determinada finalidade.
- Os Controles Internos são influenciados pela pessoas. Não existem somente políticas, manuais, formulários mas sobretudo pessoas, em todos os níveis de uma organização.
- Os Controles Internos podem fornecer somente uma razoável segurança, e não uma segurança absoluta, para a diretoria de uma corporação.
- Os Controles Internos são centrado na realização de objetivos em uma ou mais categorias que podem ser separadas ou sobrepostas.

A estrutura descrita no ICIF do COSO consiste de cinco componentes, relacionados entre si. De acordo com o COSO, estes componentes fornecem uma estrutura efetiva para descrever e analisar o sistema de controles internos usado por uma empresa.

Os componentes são os seguintes:

- Ambiente de Controle (postura da organização e conscientização das pessoas)
- Avaliação de Riscos (identificação e analise de riscos relevantes para alcançar os objetivos definidos)
- Atividades de Controle (políticas e processos em todos os níveis para garantir a observância das diretrizes e medidas de prevenção dos riscos)
- Informações e Comunicações (fluxos das informações e comunicações dentro da corporação)
- Monitoramento (Processos de monitoramento e avaliação do sistema e dos demais processos)

Os oito componentes do ERMIF (Enterprise Risk Management) compreendem os cinco anteriores (do ICIF) ao passo que expandem o modelo de estrutura, de forma a atender a maior demanda que advém da gestão de riscos corporativos:

- Ambiente interno
- Definição de objetivos
- Identificação de Eventos
- Avaliação de riscos
- Resposta a riscos
- Atividades de Controle
- Informação e Comunicação
- Monitoramento

COBIT (Control Objectives for Information and related Technology) é um conjunto de diretrizes, indicadores, processos e melhores praticas para a gestão e governança dos sistemas informáticos. O COBIT foi criado em 1996 nos EUA em conjunto pela Information Systems Audit and Control Association (ISACA) e pelo IT Governance Institute (ITGI).

O COBIT é útil para gestores de TI (Tecnologia da Informação - Information Technology), usuários e auditores, ao longo dos anos se consolidou como o padrão internacional para estruturas de governança e controle de TI.

Vale mencionar, em contraposição, as normas ISO/IEC 27002 que também representam um padrão internacional de melhores praticas em TI, mas que são focadas sobretudos na gestão da segurança das informações. O COBIT, normalmente, abrange uma área mais ampla da ISO/IEC 27002, a qual é bem centrada nas questões relativas a segurança.

O “pacote” COBIT completo, compreende os seguintes pontos:

- Sumario Executivo
- Estrutura de Governança e Controle
- Objetivos de Controle
- Diretrizes de Gestão
- Guia de Implementação
- Guia de Seguros de TI

O COBIT está hoje na versão 4.1 (existe uma versão 5, mas não definitiva) e é composto por 34 processos de alto nível os quais cobrem 210 objetivos de controle divididos nos seguintes 4 domínios:

- Planejamento e Organização
- Aquisição e Implementação
- Entrega e Suporte
- Monitoramento e Avaliação

Como integrar os frameworks COSO, COBIT e ISO 27001

Recentemente, a ISO (International Standardization Organization) atualizou a ISO 9001, ISO 14001 e a ISO 27001 para tornar mais fácil usá-las em conjunto. Mas, como elas interagem com práticas for a do mundo ISO?
Este artigo apresentará como a ISO 27001 pode ser usada com os frameworks COSO e COBIT para reduzir o esforço administrativo e aumentar os benefícios que cada um deles pode trazer às organizações.

AAL | Consultoria & Auditoria

O que é o COSO?

COSO (Committee of Sponsoring Organizations of the Treadway Commission) é uma iniciativa conjunta apoiada por cinco organizações do setor privado nos Estados Unidos para combater fraudes corporativas.

O framework COSO, atualmente na versão 2013, apoia gestores, conselhos de administração, e outras parte interessadas relevantes, desde o nível mais alto “entidade” até o mais baixo nível “função”, no entendimento sobre o que constitui um sistema de controle interno e quando um controle interno está sendo eficaz.
Ele faz isso definindo 17 princípios de controle para atingir:

- Eficácia e eficiência das operações da organização
- Confiabilidade, oportunidade e transparência dos relatórios
- Aderência a leis e regulamentações

Os 17 princípios de controle estão divididos nestes componentes:

- Ambiente de controle: normas, processos e estrutura para a execução do controle interno;
- Avaliação de risco: processo para identificação e avaliação dos riscos para o atingimento dos objetivos;
- Atividades de controle: ações para assegurar que as diretivas da gestão estão sendo executadas;
- Informação & comunicação: informação para apoiar os componentes do controle interno e comunicação para continuamente prover, compartilhar e obter a informação necessária;
- Atividades de monitoramento: avaliação para verificar se cada componente e controle está presente e funcionando.

Para lidar com a velocidade da dinâmica do negócio e necessidade por respostas rápidas, o COSO enfatiza o julgamento e o bom senso da administração, sobre rigorosa aderência a políticas e procedimentos, para a tomada de decisão.

Isto requer das partes interessadas um profundo entendimento do contexto organizacional para:

- Determinar quanto controle é o suficiente
- Selecionar, desenvolver e implementar controles em uma base diária
- Monitorar e avaliar a eficácia dos controles

O que é o COBIT?

COBIT (Control Objectives for Information and Related Technologies) é um framework para gestão e governança de TI sob responsabilidade do ISACA (Information Systems Audit and Control Association). Ele prove controle implementáveis para tecnologia da informação, organizados em processos relacionados a TI, que apoiam o cumprimento destes requisitos de negócio:

- Uso eficaz da informação, considerando relevância, tempo e condições de entrega
- Alocação eficiente de recursos
- Confidencialidade, para proteger a informação contra acesso e divulgação não autorizada
- Integridade do conteúdo da informação
- Disponibilidade quando demandada pelos processos do negócio
- Conformidade com requisitos legais
- Confiabilidade da informação usada para a tomada de decisão

O framework de processos do COBIT, atualmente na quinta versão, publicada em 2012, está dividido em quatro domínios:

- Planejar e organizar: o uso da TI para ajudar a organização a atingir seus objetivos;
- Adquirir e implementar: a aquisição de soluções de TI, a integração delas com os processos de negócio, e a manutenção requerida para assegurar que estas soluções se mantenham atendendo as necessidades de negócio;
- Entregar e suportar: foca na execução das aplicações e seus resultados de uma forma eficaz e eficiente; ele também cobre necessidades de segurança e treinamento;
- Monitorar e avaliar: provê garantia de que as soluções de TI estão atingindo seus objetivos e que estão em conformidade com as questões legais.
- Para cada processo, o COBIT define entradas, saídas, atividades chave, objetivos, e medidas de desempenho. Embora o COBIT tenha mais detalhes em termos de processos, ainda faltam detalhes técnicos para apoiar a implementação.

E sobre a ISO 27001?

A ISO 27001 é a norma ISO que descreve como gerir a segurança da informação em uma organização.
Ela consiste de 11 cláusulas na parte principal, e 114 controles de segurança agrupados em 14 seções no Anexo A.
As cláusulas da parte principal da norma ISO 27001:2013 são:

- 4 – Contexto da organização
- 5 – Liderança
- 6 – Planejamento
- 7 – Suporte
- 8 – Operação
- 9 – Avaliação do desempenho
- 10 – Melhoria contínua

O Anexo A da ISO 27001:2013 cobre controles relacionados a estrutura organizacional (física e lógica), recursos humanos, tecnologia da informação, gestão de fornecedores, etc.

Para informações detalhadas, leia: Uma primeira impressão sobre a nova ISO 27001 e Visão geral do Anexo A da ISO 27001:2013.

Uma das limitações da ISO 27001 é que ela não prove detalhes sobre o que fazer para atender os requisitos ou implementar controles, apenas o que você precisa atingir. Para detalhes, você pode usar a ISO 27002 como guia. Para mais informação, leia: Semelhanças e diferenças entre a ISO 27001 e a ISO 27002.

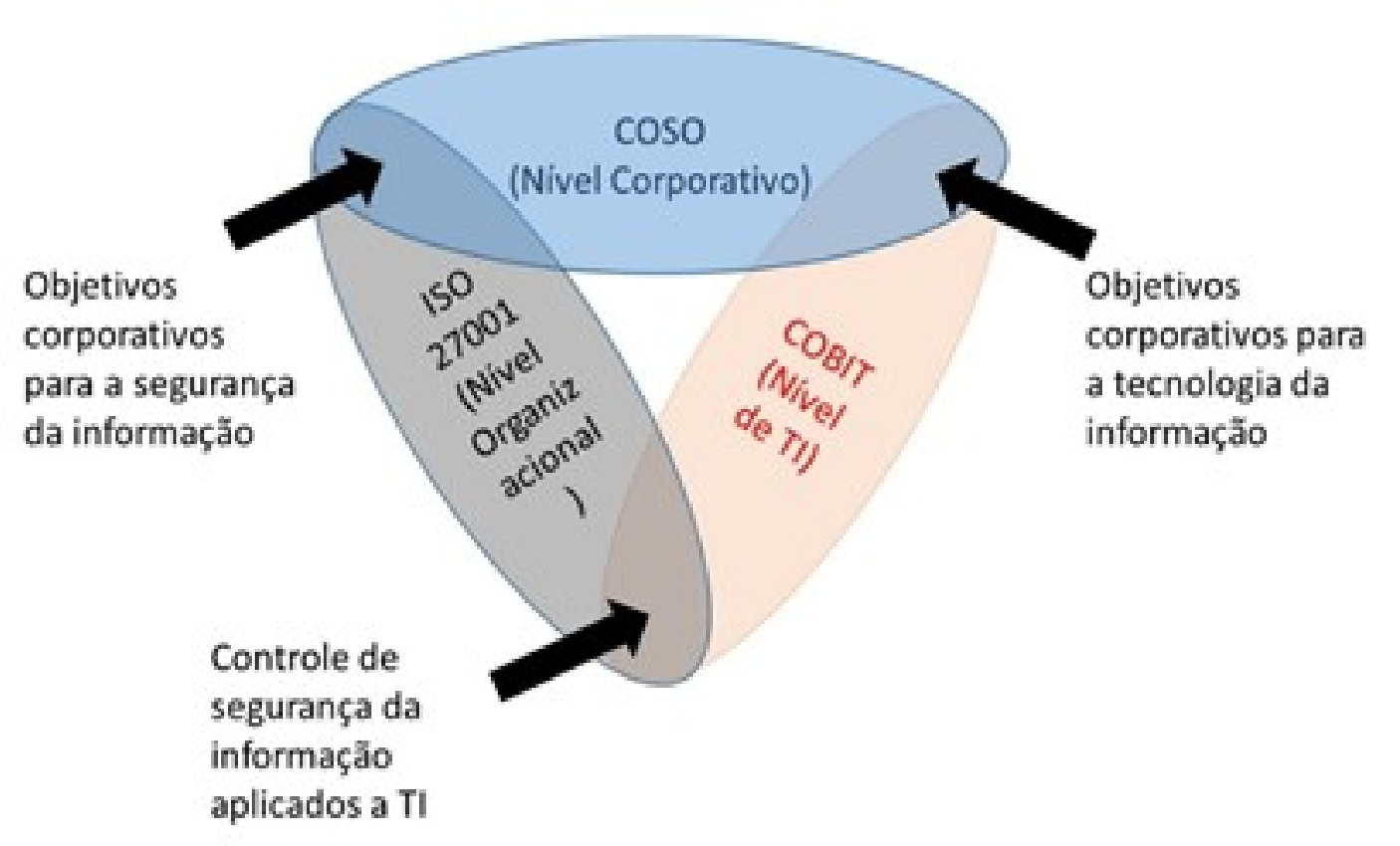
Como a ISO 27001 pode interagir com o COSO e COBIT?

Basicamente, o COSO, COBIT, e a ISO 27001 têm estes aspectos em comum:

- **Dirigidos por objetivos.** Enquanto o COSO e o COBIT possuem objetivos claramente definidos, a ISO 27001 requer que os objetivos de segurança da informação sejam definidos por cada organização de acordo com seu contexto em termos de confidencialidade, integridade e disponibilidade, para assegurar que a os processos de segurança e da organização estejam integrados.
- **Orientados a processos.** Todos os três frameworks fazem uso de uma abordagem de processo para organizar suas atividades, e isto pode ser usado para formar uma visão sistêmica de como eles podem interagir.
- **Uso de controles.** Enquanto que com o COSO os controles são mais genéricos, com o objetivo de cobrir tantos processos de negócio quanto possível, o COBIT reduz seu escopo para as tecnologias da informação, e a ISO 27001 para a segurança da informação.

Isto resulta em oportunidades para sobrepô-los e otimizar as ações.

A relação entre eles pode ser vista como:



Aqui está como eu resumiria uma possível relação entre estes três frameworks:

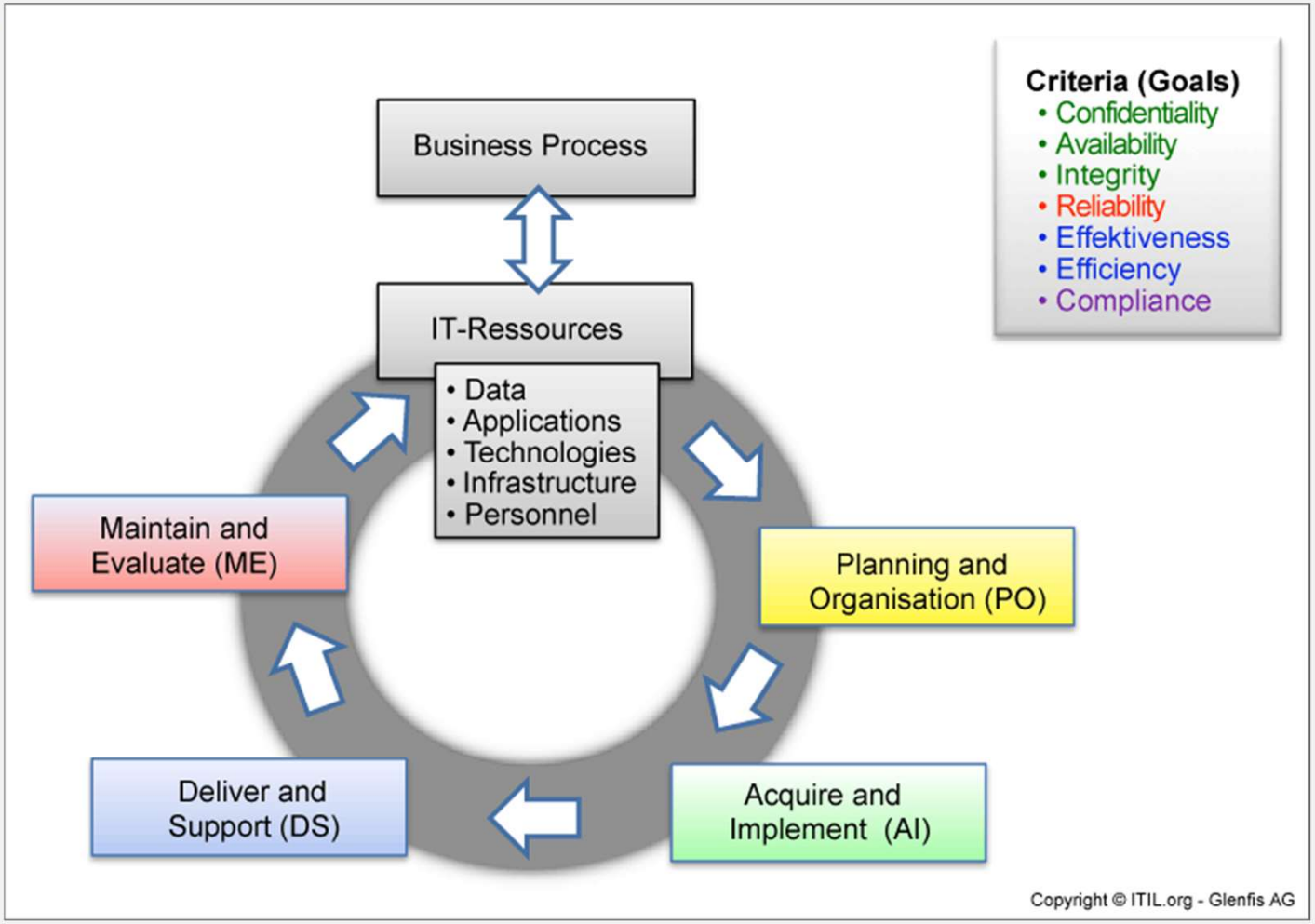
"Confiabilidade do reporte" (COSO), suportado pelo "uso eficaz da informação" (COBIT) e controle de "integridade" e "disponibilidade" (ISO 27001).

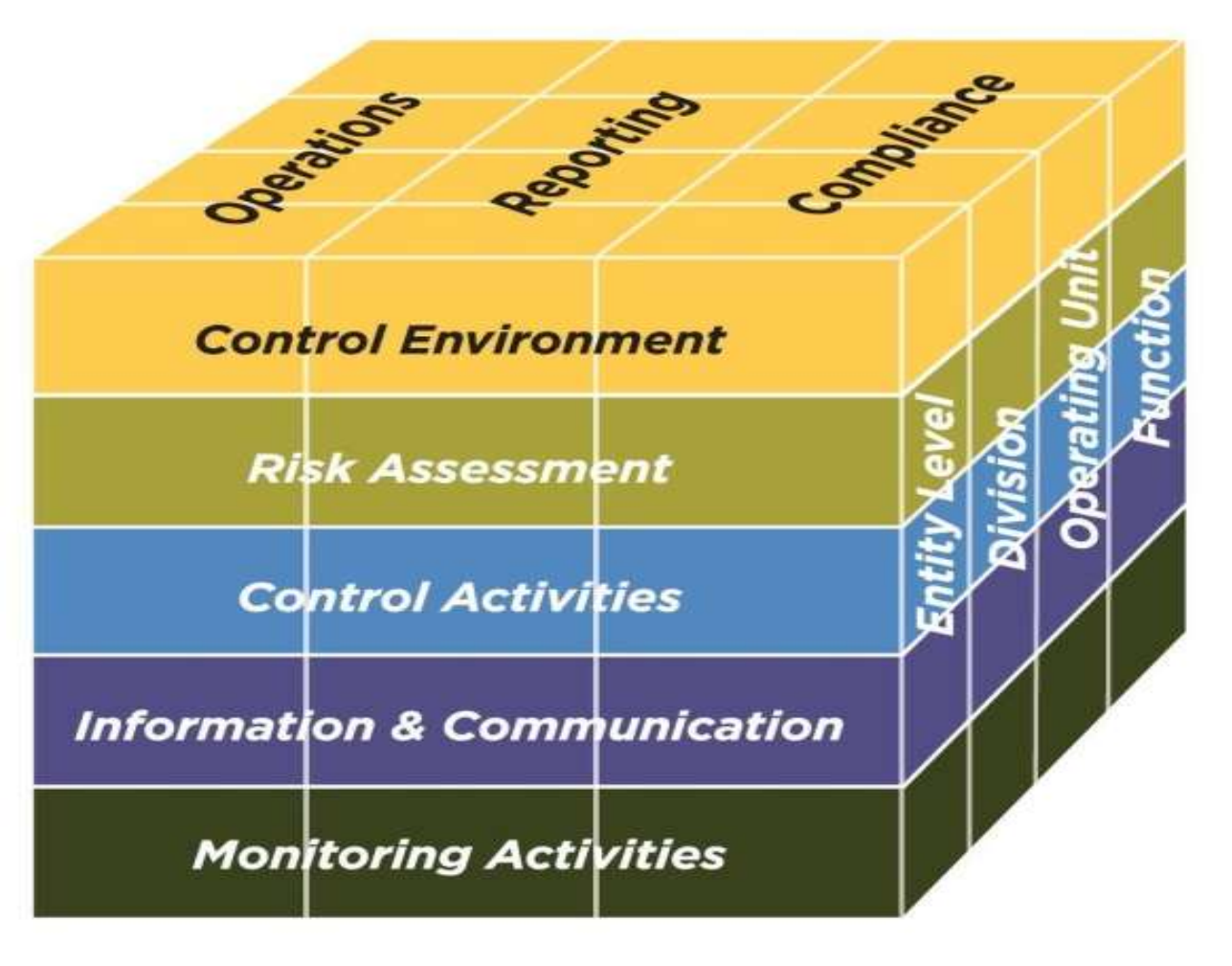
Esta relação clara simplifica enormemente o trabalho de mostrar como a segurança da informação pode ser integrada ao negócio, não apenas em um nível operacional, mas até os mais altos níveis, incluindo através de outros processos organizacionais.

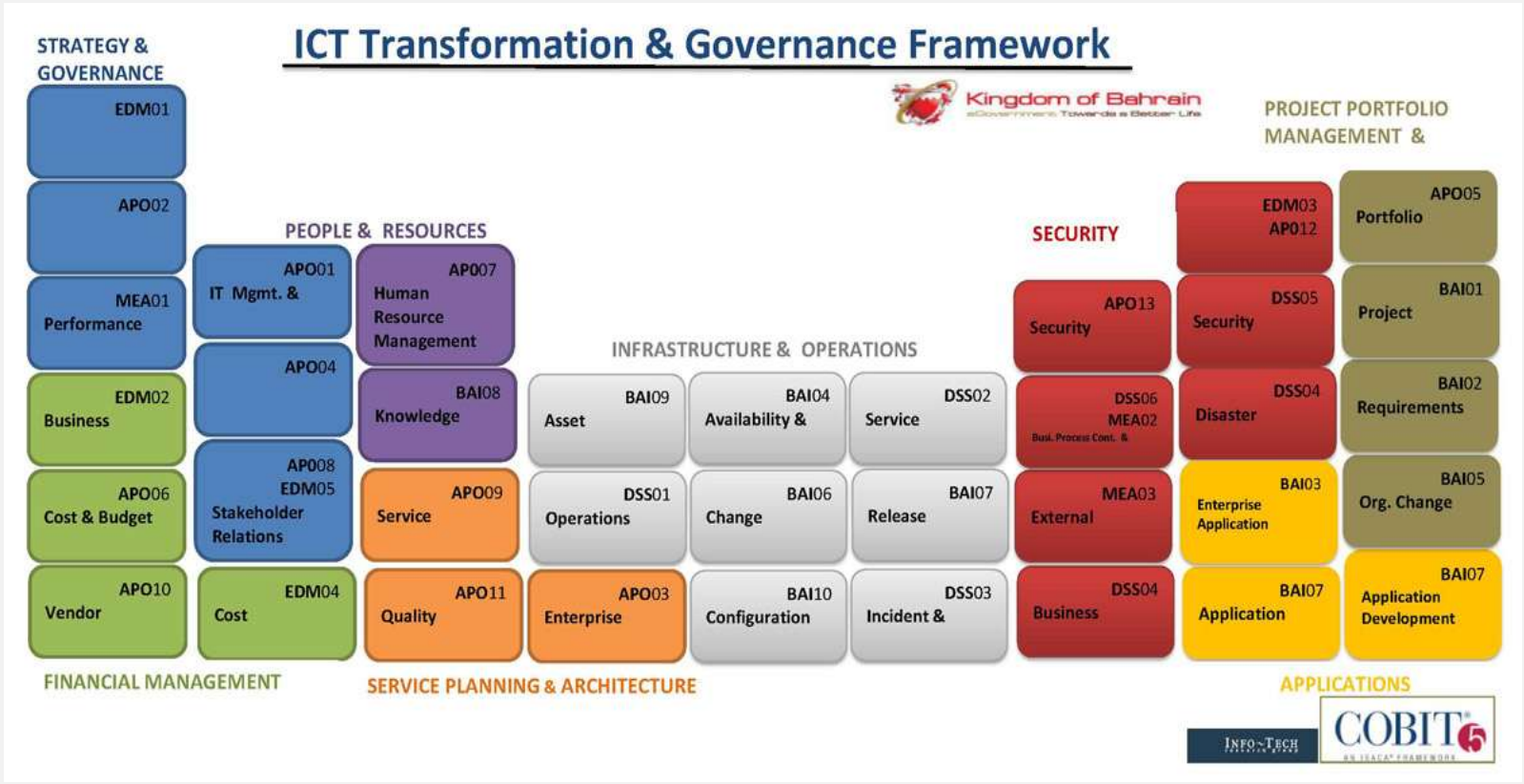
O todo é maior do que a soma de suas partes

Quando fazemos duas ou mais coisas trabalhem em conjunto de uma forma que resulta em um efeito maior do que a soma de cada contribuição individual, nós temos sinergia; e, ao entender quais aspectos da ISO 27001 podem ser usados para apoiar outros frameworks organizacionais, como o COSO e o COBIT, podemos descobrir novas formas de otimizar nossos recursos e, ao mesmo tempo, melhorar a segurança e o desempenho do negócio.

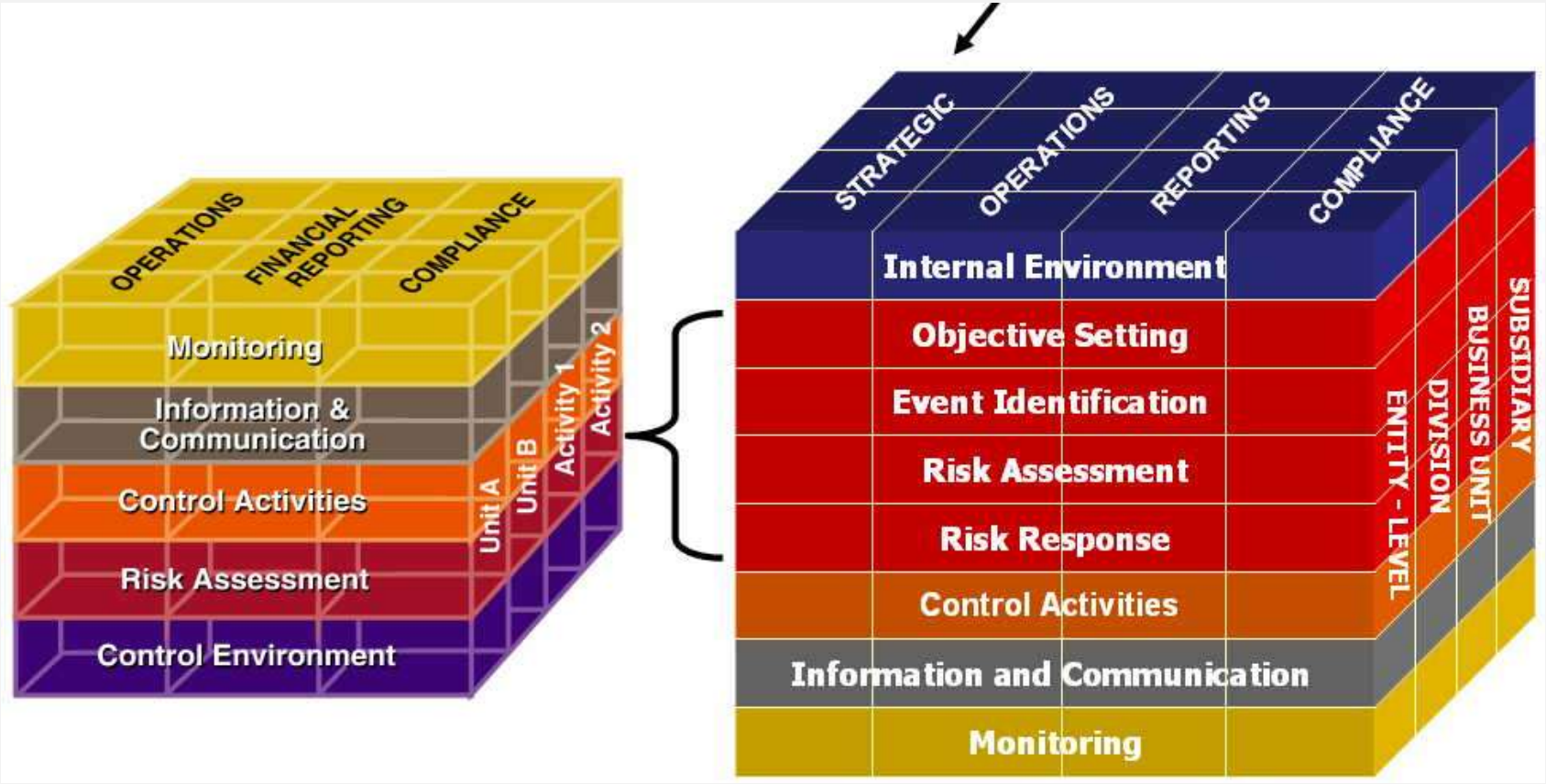
Para aprender mais sobre os requisitos da ISO 27001 e facilitar o processo de integração com outros frameworks, tente nosso treinamento online gratuito: ISO 27001:2013 Foundations Course.







AAL Consultoria & Auditoria



Soft Controls

"People"

Openness

Shared Values

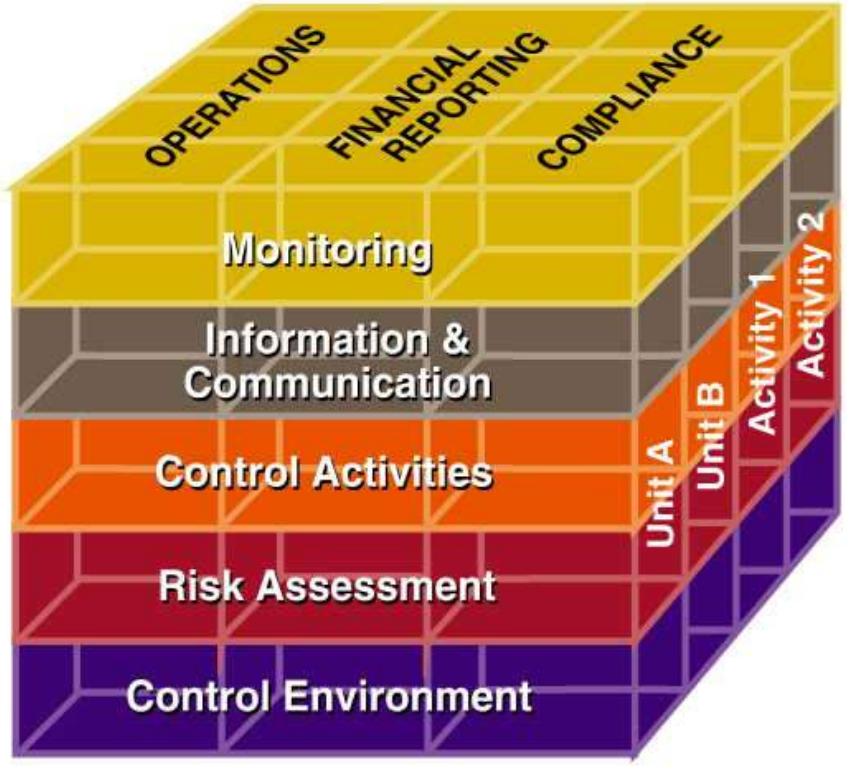
Clarity

Commitment to Competence

Honesty

High Expectations

Communications



Hard Controls

"Activities"

Reviews

Inspections

Policies

Reconciliations

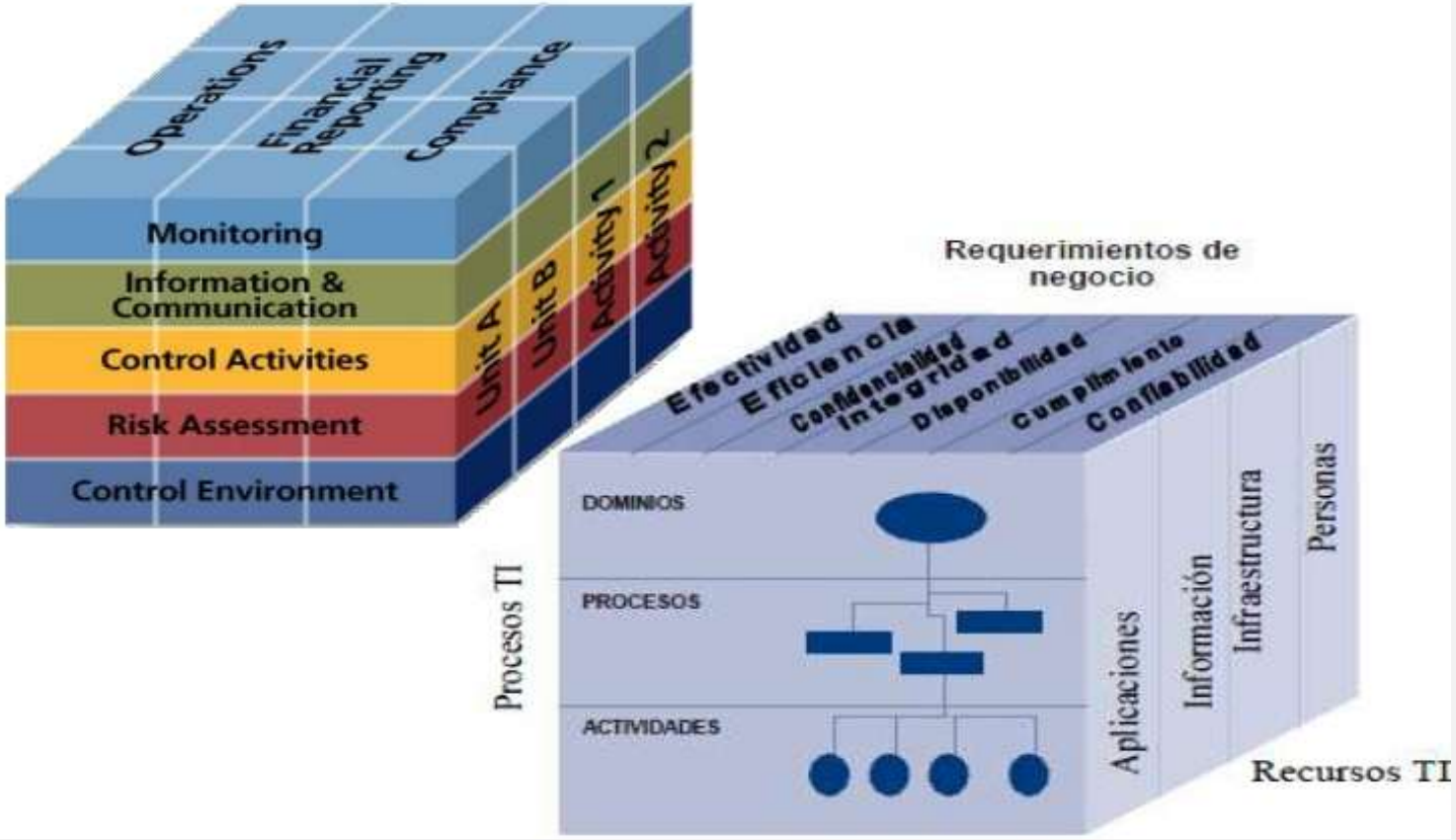
Structure

Limits of Authority

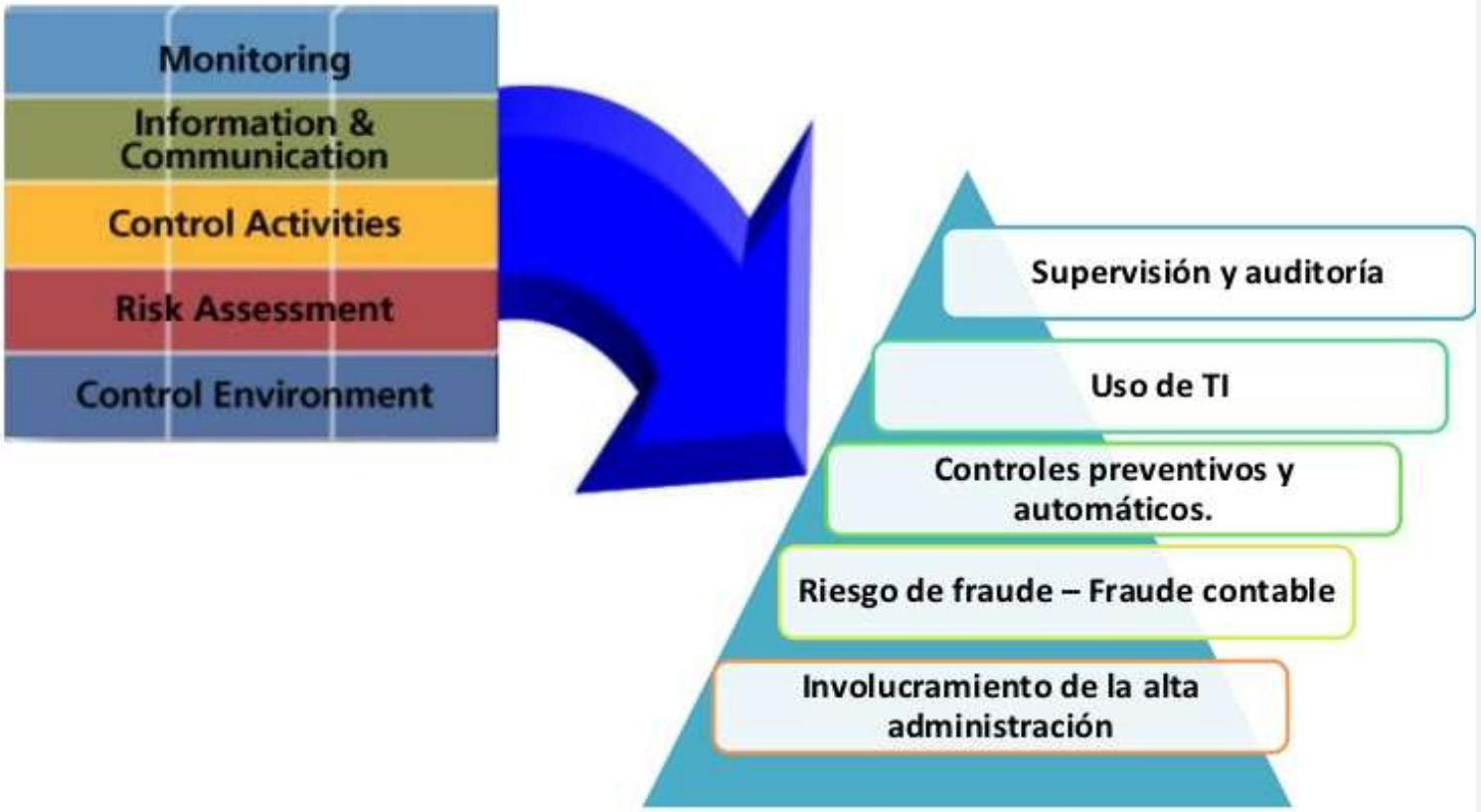
Userids and Password

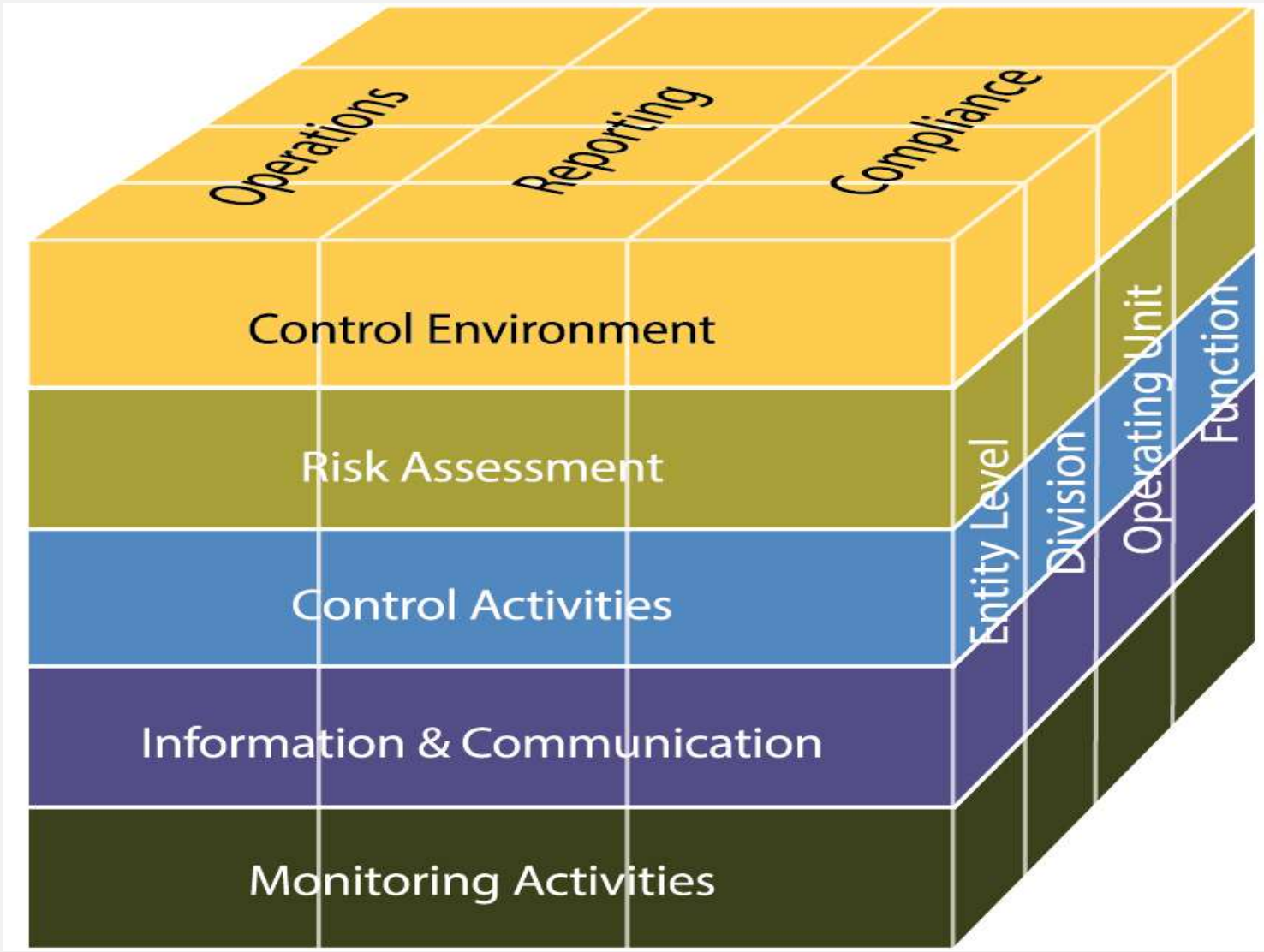
Physical Counts

COSO y COBIT

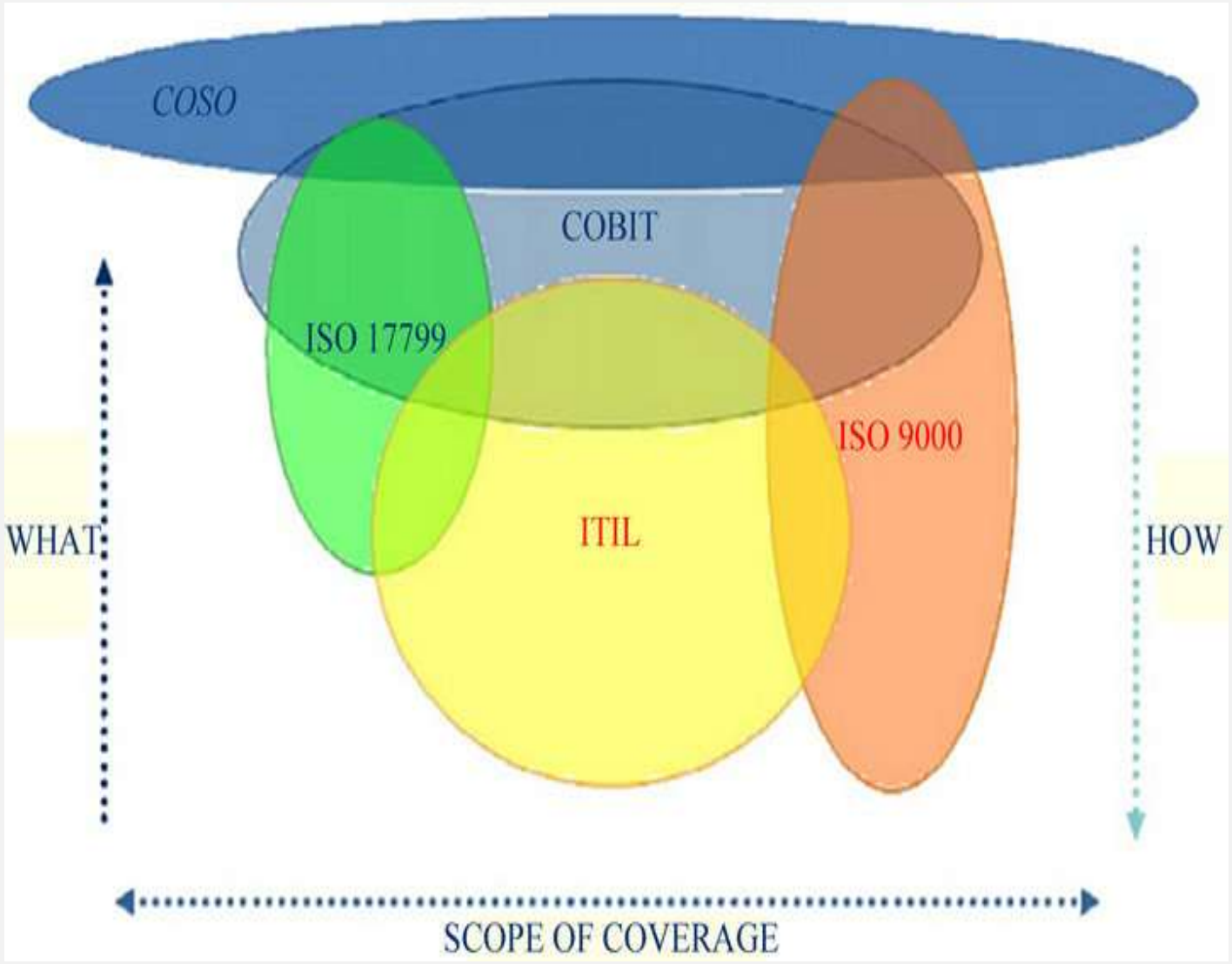


Aplicación de COSO y COBIT

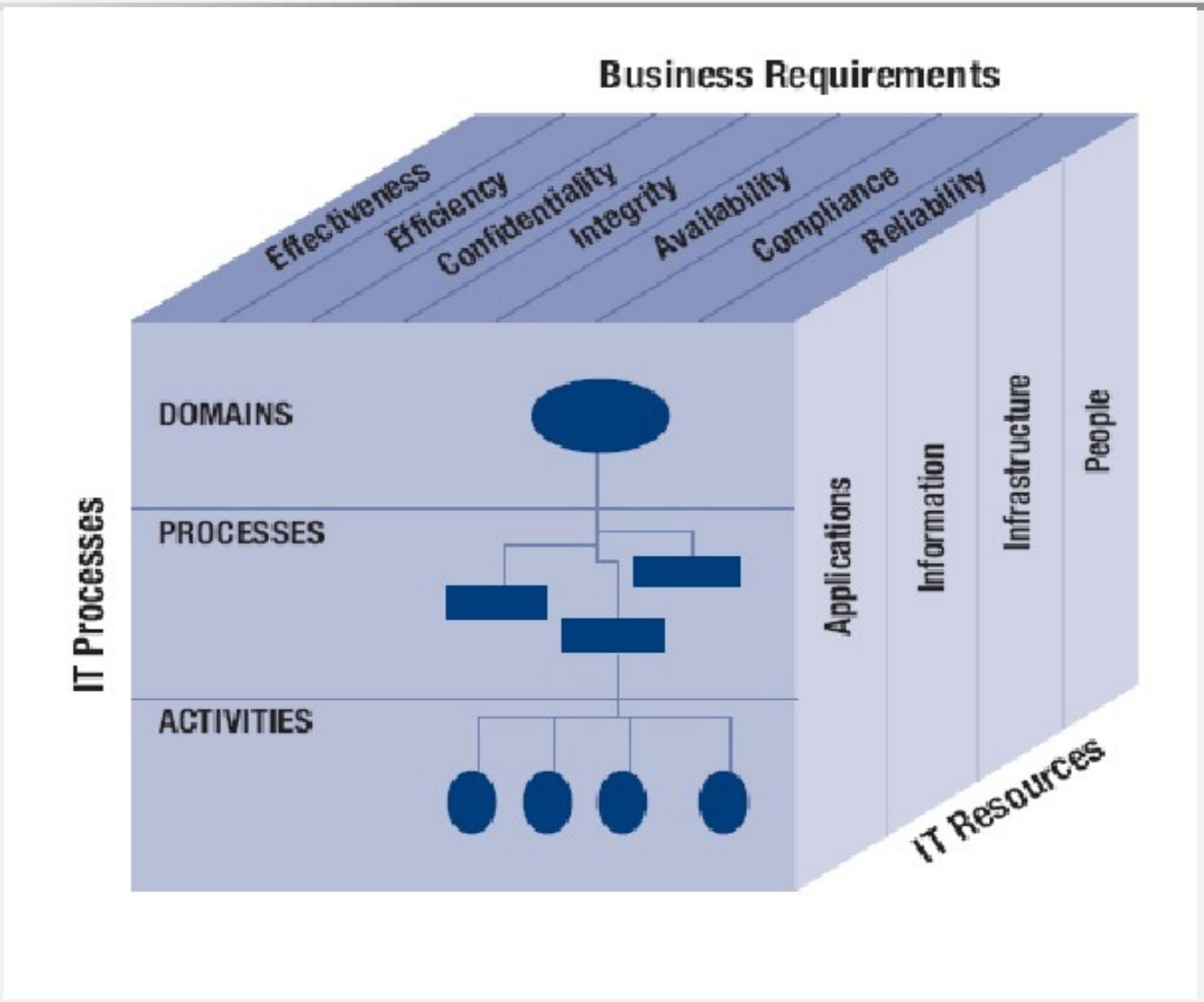




AAL Consultoria & Auditoria



AAL Consultoria & Auditoria



COSO PYRAMID

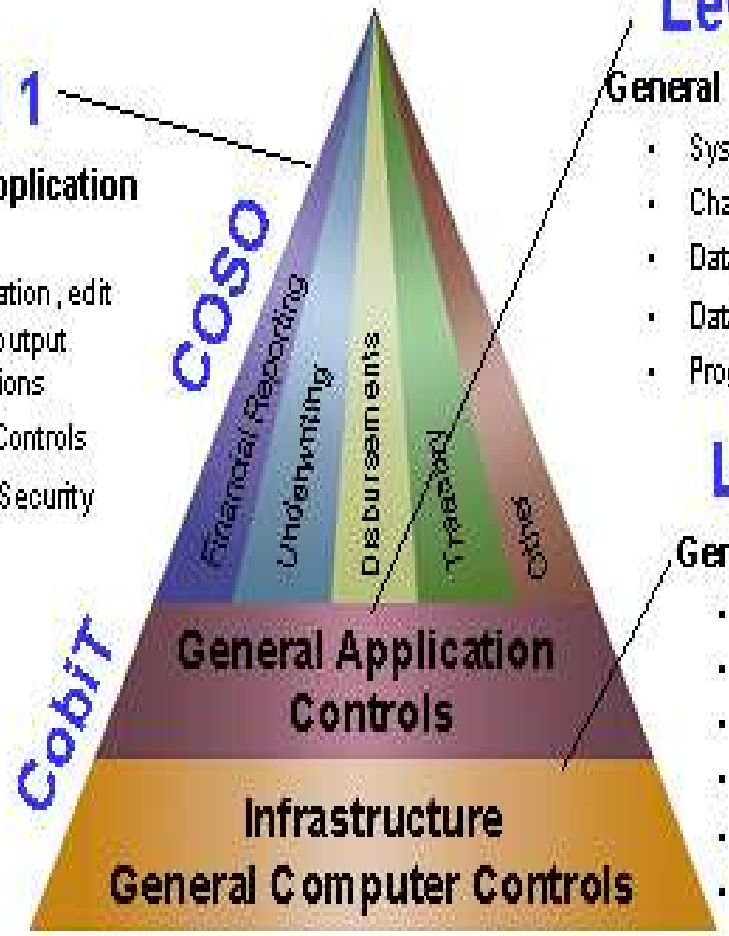
COSO CUBE

AAL | Consultoria & Auditoria

Level 1

Automated Application Controls

- Data validation, edit checks & output reconciliations
- Interface Controls
- End User Security



Level 2

General Application Controls

- System development
- Change control
- Data Recovery
- Database management
- Programmer security

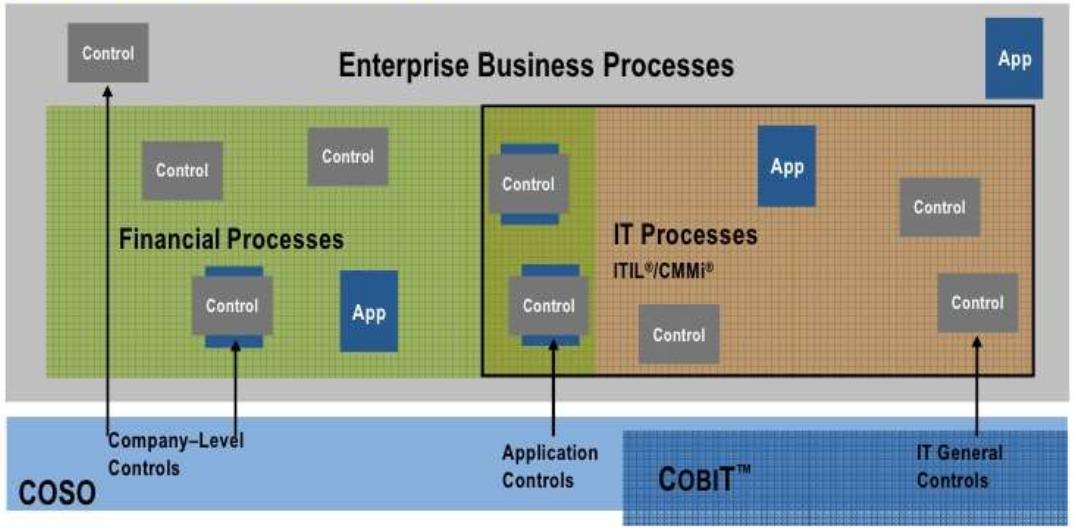
Level 3

General Computer Controls

- Change and configuration management
- Network Administration
- Security Administration
- Data center operations
- Database Administration
- Disaster Recovery
- O/S Administration

COBIT, COSO, ITIL & Compliance

Process and Control Framework



Control Frameworks:	COSO — Control and risk mgmt for corporate governance
	COBIT™— IT Control Objectives
IT Process Frameworks:	ITIL®/CMMi®—IT Best Practices

COBIT™ Trademark of ISACA
ITIL® Trademark of OGC
CMMi® Trademark of SEI

OBRIGADO

EMAIL's:
agnaldo.alves@grupoaal.com.br
contato@grupoaal.com.br

WhatsApp:
55 041 99948-2273

AAL | Consultoria & Auditoria