PEMPAL

IACOP Internal Audit Community of Practice

Avaliação da Eficácia do Controle Interno: Orientação PEMPAL: para Auditores Internos do Setor Público

outubro de 2020

Comunidade de Prática de Auditoria Interna (IACOP)
T: +7 495 745 70 00 Ramal 2002
E: IACOP@pempal.org
Site: www.pempal.org

ÍNDICE

AGRADECIMENTOS 2

O que são PEMPAL e IACOP? 3

PREFÁCIO 4

SIGLAS 5

PARTE 1. INTRODUÇÃO 6

PARTE 2. O QUE É CONTROLE INTERNO? 7

PARTE 3. APLICAÇÃO DO CONTROLE INTERNO NOS PAÍSES PEMPAL 13

PARTE 4. MODELO DE MATURIDADE DE CONTROLE INTERNO 15

Anexo A. Princípios de Controle Interno e Pontos de Foco 17

Anexo B1. O Ambiente de Controle 29

Anexo B2. Avaliação de risco 46

Anexo B3. Atividades de Controle 63

Anexo B4. Informação e Comunicação 78

Anexo B5. Monitoramento e Avaliação 92

Anexo C. Avaliação da Maturidade dos Controles Internos 101

AGRADECIMENTOS

Esta orientação foi desenvolvida pela Comunidade de Prática de Auditoria Interna (IACOP) do Grupo de Trabalho de Controle Interno da Aprendizagem Assistida por Pares de Gestão da Despesa Pública (PEMPAL). A IACOP gostaria de agradecer a todos aqueles que contribuíram, incluindo todos os membros do Grupo de Trabalho de Controle Interno da IACOP, e reconhecer, em particular, os seguintes contribuintes principais: Richard Maggs, consultor do Banco Mundial; Edit Nemeth (Hungria), ex-presidente do Comitê Executivo da IACOP (ExCom) e ex-líder do Grupo de Trabalho de Controle Interno; e Arman Vatyan, Banco Mundial, Líder do Programa PEMPAL.

O QUE SÃO PEMPAL E IACOP?

A PEMPAL é uma rede para facilitar a troca de experiência profissional e a transferência de conhecimento entre os profissionais de gestão financeira pública em países da Europa e da região da Ásia Central. A rede, lançada em 2006, visa contribuir para o fortalecimento das práticas de gestão das finanças públicas nos países membros, por meio do desenvolvimento e divulgação de boas práticas e sua aplicação.

A PEMPAL organiza-se em torno de três comunidades temáticas de prática:

- Comunidade de Prática Orçamentária,
- Comunidade de Prática do Tesouro, e
- Comunidade de Prática de Auditoria Interna (IACOP).

O principal objetivo geral da IACOP é apoiar seus países membros na estabelecer sistemas de auditoria interna modernos e eficazes que atendam aos padrões e boas práticas internacionais; importante para a boa governança e prestação de contas no setor público.

Os principais doadores e parceiros de desenvolvimento do programa são a Secretaria de Estado para Assuntos Econômicos da Suíça, o Ministério das Finanças da Federação Russa e o Banco Mundial. A Academia Nacional Holandesa de Finanças e Economia fornece apoio não financeiro.

PREFÁCIO

“Avaliar a Eficácia do Controlo Interno: Orientação PEMPAL para Auditores Internos do Sector Público” é um produto de conhecimento desenvolvido pelo IACOP para auditores internos, para auxiliar na compreensão e avaliação da eficácia do controle interno.

Outros produtos de conhecimento de boas práticas da IACOP incluem: Modelo de Manual de Auditoria Interna de Boas Práticas; Modelo de Manual de Boas Práticas de Desenvolvimento Profissional Contínuo; Corpo de Conhecimento de Auditoria Interna; Avaliação de Risco no Planejamento de Auditoria; Guia de Avaliação da Qualidade; Orientação PEMPAL sobre Auditoria Interna: Demonstrar e Medir o Valor Acrescentado; Glossário de Termos PEMPAL: Controlo Interno; O Impacto do COVID-19 no Papel e nas Atividades da Auditoria Interna; e Principais Indicadores de Desempenho para Funções de Auditoria Interna. Todos estão disponíveis em www.pempal.org.

SIGLAS

COBIT	Objetivos de Controle para Tecnologia da Informação e Relacionada
COSO	Comitê de Organizações Patrocinadoras da Comissão Treadway
IACOP	Comunidade de Prática de Auditoria Interna
IIA	Instituto de Auditores Internos
TI	Tecnologia da Informação
KPI	Indicador Chave de Desempenho
GFP	Gestão das Finanças Públicas
PEMPAL	Rede de Aprendizagem Assistida por Pares de Gestão de Despesas Públicas
PIC	Controle Interno do Setor Público
SAI	Entidade Fiscalizadora Superior

PARTE 1. INTRODUÇÃO

Esta orientação foi desenvolvida para ajudar os auditores internos a entender melhor as principais características de um controle interno eficaz e como avaliar e avaliar a funcionalidade dos sistemas de controle interno. Inclui uma série de critérios para avaliar a maturidade dos controles internos. Isso pode ser útil para auditores internos que trabalham em organizações que estão desenvolvendo/refinando sistemas de gestão financeira pública (GFP). A orientação:

- Descreve as principais características do controle interno conforme promovido pelo Comitê de Organizações Patrocinadoras da Comissão Treadway (COSO)[1] (Parte 2 e Anexo A).
- Explica os cinco componentes do controle interno e os 17 princípios subjacentes do controle interno que precisam ser atendidos para que o controle interno seja eficaz, adaptado ao contexto do setor público (Parte 3 e Anexos B1-B5).
- Identifica critérios para avaliar até que ponto cada um dos princípios foi cumprido (Anexos B1-B5).
- Promove um modelo de avaliação em quatro níveis da maturidade do controle interno (Parte 4).
- Apresenta um quadro detalhado de avaliação da maturidade dos controles internos aos quatro níveis, com base nos critérios de avaliação do PEMPAL (Anexo C).

Esta orientação será usada pela IACOP e pode ser atualizada para refletir as opiniões expressas e o conhecimento desenvolvido em futuras reuniões do Grupo de Trabalho de Controle Interno.

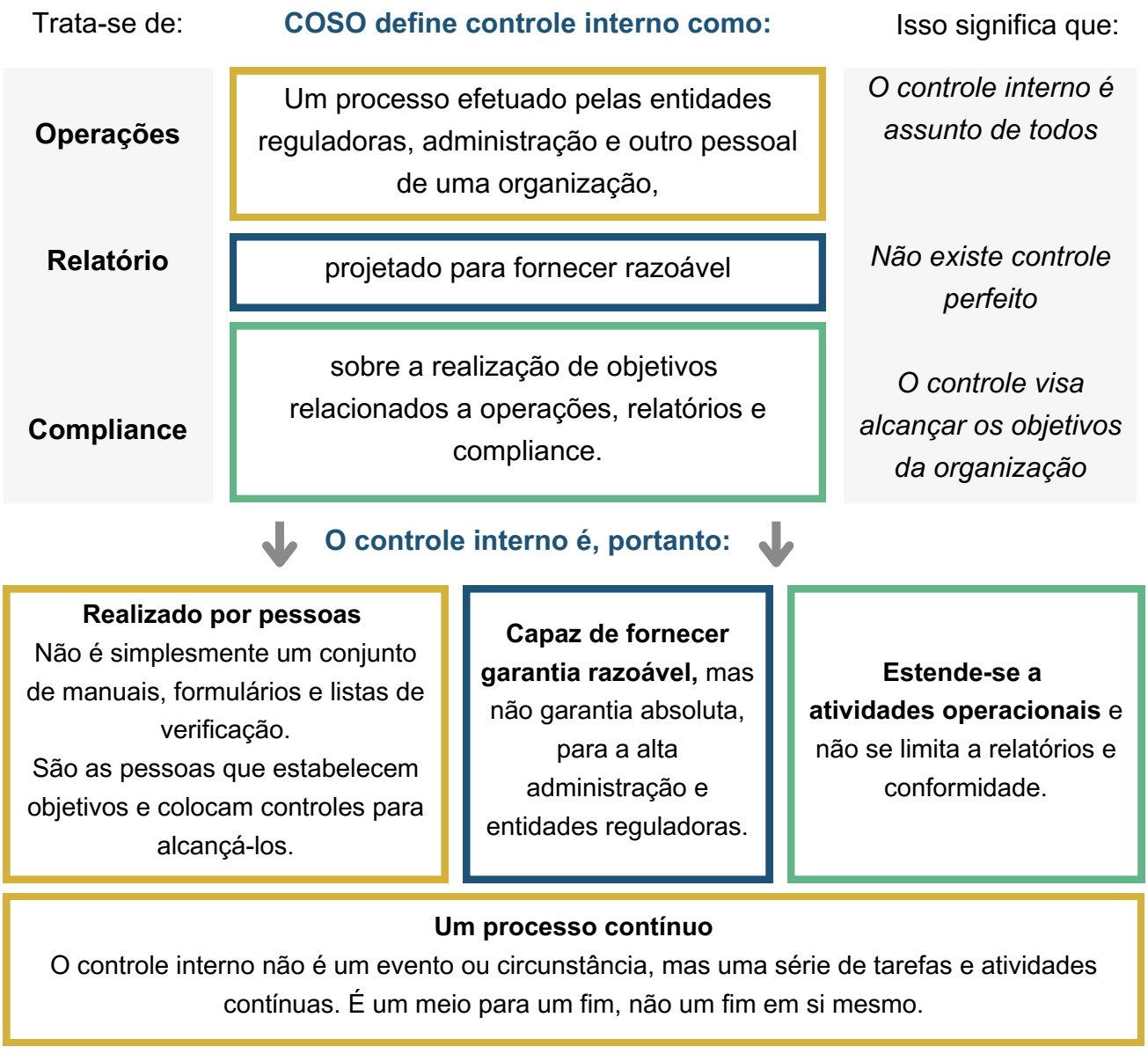
[1] COSO é uma iniciativa global para desenvolver estruturas e orientações sobre gerenciamento de riscos corporativos, controle interno e dissuasão de fraudes. https://www.coso.org/Pages/default.aspx

PARTE 2. O QUE É CONTROLE INTERNO?

A definição de controle interno

O COSO define controle interno como "Um processo, executado pelos órgãos administrativos de uma organização,[2] administração e outro pessoal, projetado para fornecer garantia razoável em relação ao alcance dos objetivos relacionados a operações, relatórios e conformidade."[3] A Figura 1 ilustra como essa definição pode ser interpretado para uso em países PEMPAL.

Figura 1. A definição de controle interno explorada

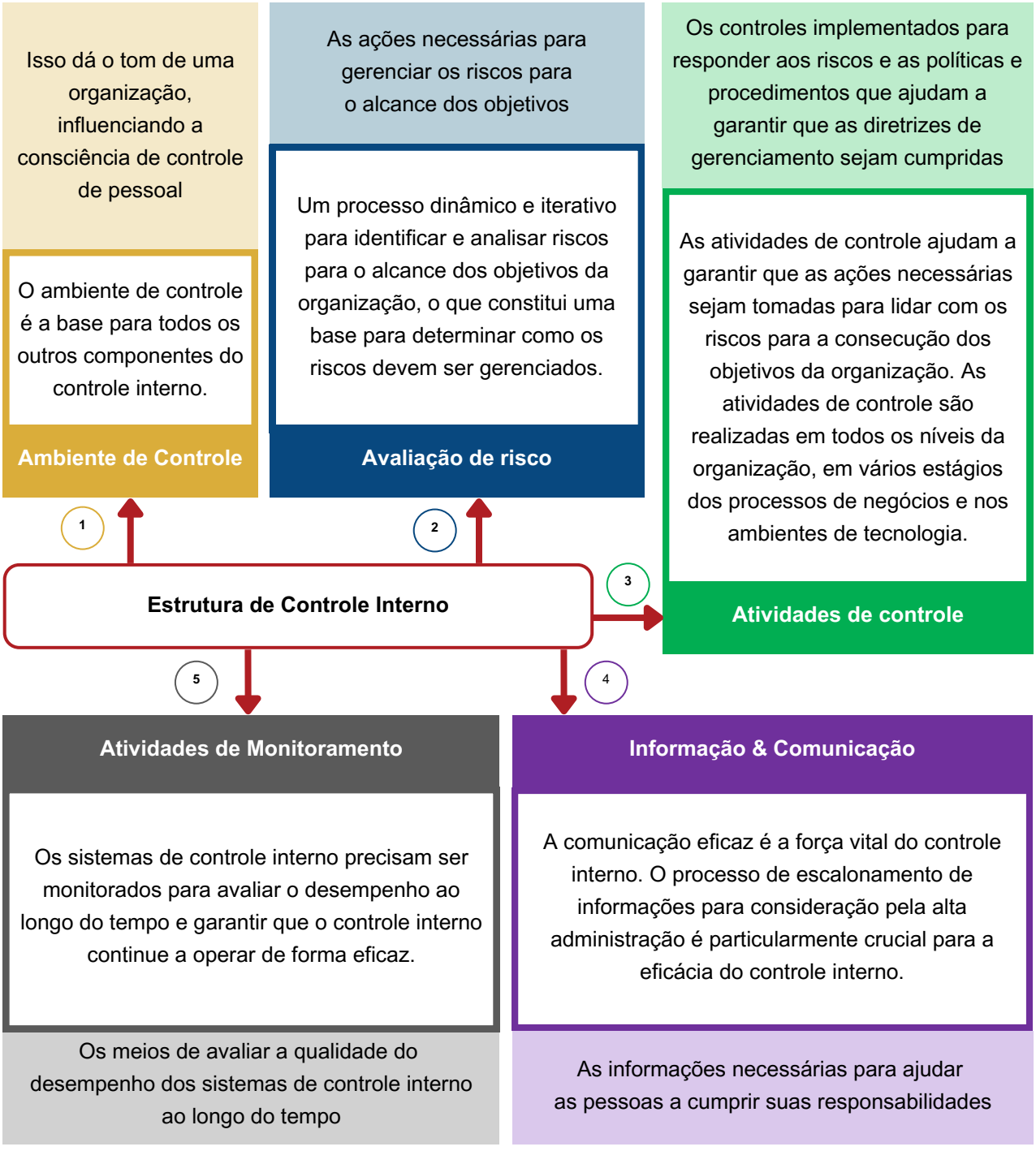


2. A palavra "conselho" conforme usada no COSO pode ser traduzida no setor público como a entidade ou entidades responsáveis por fornecer governança e supervisão da organização do setor público em questão ou entidades reguladoras. Em alguns países (por exemplo, Reino Unido) essa função de governança é desempenhada por um conselho de administração independente.
3. COSO. "Controle Interno - Estrutura Integrada", 2013

Os principais componentes do controle interno

O COSO reconhece cinco componentes inter-relacionados de controle interno: ambiente de controle, avaliação de risco, atividades de controle, informação e comunicação e atividades de monitoramento. Esses cinco componentes, mostrados na Figura 2 abaixo, precisam estar implementados e integrados para serem eficazes nos objetivos operacionais, de relatórios e de conformidade.

Figura 2. Os cinco componentes do controle interno



O controle interno não é um processo no qual um componente afeta apenas o próximo. É um processo multidirecional no qual quase qualquer componente pode e irá influenciar outro.

O COSO desenvolveu 17 princípios (listados e descritos no Anexo A) que devem estar presentes e funcionando para atender aos cinco componentes do controle interno. Os componentes e princípios relacionados são discutidos mais adiante na parte 3 e explicados em detalhes nos Anexos B1-B5.

Limitações do controle interno: O conceito de garantia razoável

O controle interno é um processo de fornecer segurança razoável sobre o alcance dos objetivos.

O controle interno ajuda uma organização a atingir seus objetivos estratégicos, produzir informações financeiras e de desempenho confiáveis e cumprir os regulamentos relevantes. No entanto, o controle interno não pode transformar um gestor ruim em bom, nem pode influenciar fatores externos ou restrições operacionais severas que possam impactar significativamente as operações da organização, por exemplo, a pandemia do COVID-19.

As limitações inerentes do controle interno podem incluir julgamento humano falho na tomada de decisões; erros e erros humanos simples; e a necessidade de equilibrar o custo dos controles com os riscos e benefícios envolvidos. Os controles internos também podem fornecer proteção limitada em certas situações relacionadas a ações fraudulentas, como conluio entre dois ou mais indivíduos.

O objetivo do controle interno é fornecer segurança razoável de que a organização alcançará seus objetivos. Não seria desejável nem possível que os sistemas de controle interno fornecessem garantia absoluta de que uma organização alcançaria todos os seus objetivos.

Os controles internos precisam estar "funcionando no presente" e "operando juntos"

O COSO esclarece os requisitos para um controle interno eficaz: cada um dos 5 componentes e 17 princípios relevantes devem estar **presentes e funcionando** e os 5 componentes **devem operar juntos**.

A frase “presente e funcionando” se aplica tanto aos componentes quanto aos princípios.

- “Presente” refere-se à determinação de que componentes e princípios relevantes existem no projeto e implementação do sistema de controle interno para alcançar os objetivos especificados.
- “Funcionamento” refere-se à determinação de que componentes e princípios relevantes continuem a existir na condução do sistema de controle interno para atingir os objetivos especificados.

“Operando juntos” refere-se à determinação de que todos os cinco componentes reduzam coletivamente, a um nível aceitável, o risco de não alcançar um objetivo.

Fornecer garantia sobre a eficácia do controle interno usando o modelo de três linhas

Não existe uma maneira única ou direta de avaliar a eficácia do sistema de controle interno de uma organização. O controle interno precisa estar presente e funcionando em todos os níveis da organização e em todos os processos de negócios. Todos que trabalham na organização implementam controles internos de uma forma ou de outra. Além disso, o controle interno deve ser continuamente revisado.

Muitas organizações usam o modelo de três linhas[4] (Figura 3), que identifica as várias funções do corpo diretivo, gerenciamento sênior e operacional, funções de risco e conformidade e auditoria interna para garantir que os controles internos estejam presentes e funcionando.

[4] Com base no artigo do Instituto de Auditores Internos (IIA) O MODELO DE TRÊS LINHAS - Uma atualização das Três Linhas de Defesa, julho de 2020

Figura 3. O modelo de três linhas

Sob este modelo:

- A gestão operacional fornece a primeira linha de defesa através da implementação de controles internos em seu trabalho diário;
- As funções de gerenciamento que supervisionam o risco, o controle e a conformidade fornecem a segunda linha de defesa; e
- Funções independentes, especificamente auditoria interna, fornecem a terceira linha de defesa.

PARTE 3. APLICAÇÃO DO CONTROLE INTERNO NOS PAÍSES PEMPAL

Esta orientação visa apoiar os auditores internos do setor público nos países PEMPAL a implementar sistemas eficazes de controle interno utilizando a estrutura desenvolvida pelo COSO. Esta seção descreve como usar o material detalhado contido nos anexos para conseguir isso. Cada país precisará garantir que o sistema que desenvolve seja consistente com sua estrutura legal.

Entendendo o controle interno: Os pontos de foco

Para explicar melhor os princípios dos cinco componentes, o COSO identificou detalhes explicativos sobre cada um deles, conhecidos como “pontos de foco” na orientação do COSO.

O **Anexo A** estabelece cada um dos 17 princípios e os pontos de foco relacionados.

Entendendo o controle interno: interpretando os princípios

Para ajudar os auditores internos a interpretar e aplicar os cinco componentes e 17 princípios de controle interno, os **Anexos B1 a B5** fornecem para cada componente:

- a. Um diagrama para cada princípio ilustrando como os pontos de foco podem ser interpretados.
- b. Um breve comentário sobre o propósito e as principais características de cada princípio.
- c. Um conjunto de critérios para avaliar a eficácia do controle interno desenvolvido pelo Grupo de Trabalho de Controle Interno da IACOP.

Aplicação dos princípios COSO no setor público nos países PEMPAL

Uma questão importante a ser considerada na aplicação dos princípios do COSO ao setor público nos países PEMPAL é a necessidade de adequação ao quadro legal em vigor.

Nos países anglófonos, o sistema legal permite a simples adoção de um conjunto de princípios do COSO por meio de uma legislação que permite aos gestores seguir as orientações emitidas pelo COSO. No entanto, em muitos países PEMPAL, o sistema jurídico exige que sejam atribuídos mandatos legais muito específicos ao pessoal do sector público.

Consequentemente, pode ser necessário enquadrar os princípios e conselhos do COSO como uma forma de norma ou regulamento interno para que sejam consistentes com a estrutura legal de cada país. Por exemplo:

- **Na Moldávia**, eles foram enquadrados como um conjunto de normas de controle interno que têm força legal por meio de sua publicação no Diário Oficial.
- **Na Geórgia**, todos os cinco componentes do COSO são identificados na “Lei de Controle Financeiro Interno do Estado”, que obriga os chefes das organizações estatais a garantir o desenvolvimento, a formação e a operação dos componentes de gerenciamento e controle financeiro. Existe adicionalmente uma instrução sobre a implementação dos requisitos desta lei, que também se refere ao COSO 2013.

PARTE 4. MODELO DE MATURIDADE DO CONTROLE INTERNO

As administrações públicas dos países membros da PEMPAL encontram-se em diferentes níveis de maturidade. Por esta razão, a IACOP decidiu desenvolver um modelo genérico para avaliar a maturidade (ou capacidade) do controle interno. Depois de pesquisar uma série de modelos de maturidade desenvolvidos para diferentes elementos do crescimento organizacional, a IACOP decidiu por um modelo de quatro níveis para evitar um viés para selecionar o ponto médio da escala. As características dos quatro níveis são apresentadas na Tabela 1 abaixo.

Tabela 1. Um modelo de quatro níveis para avaliar a maturidade do controle interno[5]

Nível	Características
Nível 1: Informal *Ad-hoc / Caótico*	As características dos controles internos neste nível são que eles são (normalmente) não documentados e estão em um estado de mudança dinâmica. Eles são conduzidos de maneira ad hoc, descontrolada e reativa pelos usuários aos eventos. Isso fornece um ambiente caótico ou instável para o controle interno
Nível 2: Definido *Padrão / Repetível*	As características neste nível de maturidade são que alguns controles internos estão em vigor e são repetíveis, possivelmente com resultados consistentes. É improvável que a disciplina de controle interno seja rigorosa, mas, quando existe, pode ajudar a garantir que os controles internos sejam mantidos durante períodos de estresse. Com o tempo, conjuntos de processos de controle padrão definidos e documentados serão estabelecidos e sujeitos a melhorias. **Esse pode ser um estágio de desenvolvimento demorado e é o nível em que a maioria das organizações provavelmente ficará.**

[5] Com base em um artigo de liderança de pensamento da Weaver & Tidwell LLP sobre a determinação de níveis de maturidade para controle interno, 16 de setembro de 2015.

Nível	Características
Nível 3: Gerenciado e Monitorado *Previsível*	Nesse nível de maturidade, a maioria dos controles internos é repetível e gera resultados consistentes. A disciplina de controle interno é rigorosa e garante que os controles internos sejam mantidos em momentos de estresse. Existem processos padrão projetados e documentados e o foco é melhorar continuamente o desempenho do controle interno por meio de mudanças e melhorias incrementais e inovadoras.
Nível 4: Otimizado ***Eficiente* / *Eficaz***	As características do controle interno neste nível são que a eficácia do controle interno é medida e comparada com as melhores práticas para garantir um forte desempenho em diferentes situações.

O Anexo C apresenta uma estrutura detalhada para avaliar a maturidade do controles nos quatro níveis de maturidade identificados acima. Faz isto baseando-se nos critérios desenvolvidos pela PEMPAL para cada princípio e ponto de enfoque, conforme apresentado nos Anexos B1-B5.

Embora teoricamente seja possível atribuir uma pontuação numérica (1 a 4) a cada ponto de foco para obter uma pontuação geral do nível de maturidade, isso só seria relevante se cada ponto de foco fosse igualmente importante. Este não é o caso. Avaliações de maturidade, portanto, dependem de julgamentos da importância relativa de cada ponto de foco.

ANEXO A. PRINCÍPIOS DE CONTROLE INTERNO E PONTOS DE FOCO

O COSO forneceu orientação para cada um dos 17 princípios, incluindo detalhes de suporte que ele chama de “pontos de foco”. Este anexo descreve os 17 princípios junto com os pontos de foco que podem ser relevantes para entender a aplicação de cada princípio no setor público.

Ambiente de controle

1. A organização demonstra compromisso com a integridade e valores éticos.

- **1.1. Define o tom no topo.** As entidades reguladoras e a administração em todos os níveis demonstram por meio de suas diretrizes, ações e comportamento a importância da integridade e dos valores éticos para apoiar o funcionamento do sistema de controles internos. Há consistência de mensagens sobre ética e integridade entre os níveis político e operacional do setor público.

- **1.2. Estabelece padrões de conduta.** As expectativas das entidades reguladoras e da alta direção quanto à integridade e aos valores éticos são definidas nos padrões de conduta da organização e compreendidas em todos os níveis da organização e por prestadores de serviços terceirizados e parceiros de negócios.

- **1.3. Verifica o cumprimento das normas de conduta.** Existem processos para avaliar o desempenho de indivíduos e equipes em relação aos padrões de conduta esperados da organização.

- **1.4. Aborda os desvios prontamente.** Desvios dos padrões de conduta esperados da organização são identificados e corrigidos de maneira oportuna e consistente

2. O conselho demonstra independência da administração e supervisiona o desenvolvimento e desempenho do controle interno.

- **2.1. Estabelece responsabilidades de supervisão.** As entidades reguladoras identificam e aceitam as suas responsabilidades de supervisão em relação aos requisitos e expectativas estabelecidos.

- **2.2. Tem acesso a habilidades relevantes.** As entidades reguladoras definem, mantêm e avaliam periodicamente as habilidades e conhecimentos necessários entre seus membros para capacitá-los a fazer perguntas investigativas à alta administração e a tomar medidas adequadas.

- **2.3. Opera de forma independente.** As entidades reguladoras têm membros suficientes, independentes da gestão e objetivos nas avaliações e tomadas de decisão.

- **2.4. Fornece supervisão do sistema de controle interno.** As entidades reguladoras mantêm a responsabilidade de supervisão do projeto, implementação e condução do controle interno pela administração.
- **Por exemplo:** **Ambiente de controle:** estabelecimento de integridade e valores éticos, estruturas de supervisão, autoridade e responsabilidades, expectativas de competência e prestação de contas ao conselho. **Avaliação de risco:** supervisionar a avaliação da administração dos riscos para a consecução dos objetivos, incluindo o impacto potencial de mudanças significativas, fraude e anulação do controle interno pela administração. **Atividades de controle:** fornecer supervisão à alta administração no desenvolvimento e desempenho das atividades de controle. **Informação e comunicação:** analisando e discutindo informações relacionadas ao alcance dos objetivos da organização. **Atividades de monitoramento:** avaliar e supervisionar a natureza e o escopo das atividades de monitoramento e avaliação da gestão e remediação de deficiências.

3. A administração, com a supervisão do conselho, estabelece estruturas, linhas de subordinação e autoridades e responsabilidades apropriadas na busca dos objetivos.

- **3.1. Considera todas as estruturas da organização.** A administração e os entidades reguladoras consideram as múltiplas estruturas utilizadas (incluindo unidades operacionais, distribuição geográfica e prestadores de serviços terceirizados) para apoiar o alcance dos objetivos.

- **3.2. Estabelece linhas de reporte.** A administração projeta e avalia linhas de relatórios para cada estrutura organizacional para permitir a execução de autoridades e responsabilidades e fluxo de informações para gerenciar as atividades da organização.

- **3.3. Define, atribui e limita autoridades e responsabilidades.** A administração e os entidades reguladoras delegam autoridade, definem responsabilidades e usam processos e tecnologia apropriados para atribuir responsabilidades e segregar funções conforme necessário nos vários níveis da organização:

- **Órgãos dirigentes** – retêm a autoridade sobre as decisões importantes e revisam as atribuições de gestão e as limitações das autoridades e responsabilidades;

- **Alta administração** – estabelece diretrizes, orientação e controle para permitir que a administração e outros colaboradores entendam e executem suas responsabilidades de controle interno;

- **Gerência** – orienta e facilita a execução das diretrizes da alta direção da organização e suas subunidades;

- **Pessoal** - compreender os padrões de conduta da organização, os riscos avaliados para os objetivos e as atividades de controle relacionadas em seus respectivos níveis da organização, o fluxo esperado de informações e comunicações e as atividades de monitoramento relevantes para o alcance dos objetivos;

- **Prestadores de serviços terceirizados** - Aderir à definição da administração do escopo de autoridade e responsabilidade para todos os não colaboradores contratados pela organização.

4. A organização demonstra um compromisso para atrair, desenvolver e reter indivíduos competentes em alinhamento com os objetivos.

- **4.1. Estabelece políticas e procedimentos.** As políticas e procedimentos refletem as expectativas de competência necessárias para apoiar o alcance dos objetivos.

- **4.2. Avalia a competência e aborda as deficiências.** As entidades reguladoras e a gestão avaliam as competências de toda a organização e dos prestadores de serviços subcontratados em relação às políticas e práticas estabelecidas e agem conforme necessário para colmatar as deficiências.

- **4.3. Atrai, desenvolve e retém indivíduos.** A organização fornece orientação e treinamento necessários para atrair, desenvolver e reter pessoal suficiente e competente e prestadores de serviços terceirizados para apoiar a realização dos objetivos.

- **4.4. Planeja e se prepara para a sucessão**. A alta administração e os entidades reguladoras desenvolvem planos de contingência para atribuição de responsabilidades importantes para o controle interno.

5. A organização responsabiliza os indivíduos por seu controle interno responsabilidades na prossecução dos objetivos.

- **5.1. Impõe a prestação de contas por meio de estruturas, autoridades e responsabilidades.** A administração e os entidades reguladoras estabelecem mecanismos para comunicar e responsabilizar os indivíduos pelo desempenho das responsabilidades de controle interno em toda a organização e implementar ações corretivas conforme necessário.

- **5.2. Estabelece medidas de desempenho, incentivos e recompensas.** A administração e os entidades reguladoras estabelecem medidas de desempenho, incentivos e outras recompensas apropriadas para as responsabilidades em todos os níveis da organização, refletindo as dimensões apropriadas de desempenho e os padrões esperados de conduta e considerando a consecução de objetivos de curto e longo prazo.

- **5.3. Avalia medidas de desempenho, incentivos e recompensas por relevância contínua.** A administração e os entidades reguladoras alinham incentivos e recompensas com o cumprimento das responsabilidades de controle interno, desenvolvem medidas de desempenho e avaliam o desempenho.

- **5.4. Considera pressões excessivas.** A administração e os entidades reguladoras avaliam e ajustam as pressões associadas ao alcance dos objetivos à medida que atribuem responsabilidades, desenvolvem medidas de desempenho e avaliam o desempenho.

- **5.5. Avalia o desempenho e recompensa ou disciplina os indivíduos.** Os gestores e os entidades reguladoras avaliam o desempenho das responsabilidades de controle interno, incluindo a adesão aos padrões de conduta e níveis esperados de competência e fornecem recompensas ou exercem ação disciplinar conforme apropriado.

6. A organização especifica os objetivos com clareza suficiente para permitir a identificação e avaliação dos riscos relacionados aos objetivos.

6.1. Objetivos de operações

- **Reflete as escolhas da administração:** os objetivos operacionais refletem as escolhas da administração sobre a estrutura e o desempenho da organização.
- **Considera tolerâncias de risco:** a administração considera os níveis aceitáveis de variação em relação ao alcance dos objetivos das operações.
- **Inclui metas operacionais e de desempenho financeiro:** a organização reflete o nível desejado de operações e desempenho financeiro para a organização dentro dos objetivos operacionais.
- **Forma uma base para comprometer recursos:** a administração usa os objetivos operacionais como base para alocar os recursos necessários para atingir as operações desejadas e o desempenho financeiro.

6.2. Objetivos de relatórios externos

- **Cumpre com as normas contábeis aplicáveis:** os objetivos dos relatórios financeiros são consistentes com os princípios contábeis adequados e disponíveis para a organização. Os princípios contábeis selecionados são apropriados nas circunstâncias.
- **Considera a materialidade:** a administração considera a materialidade na apresentação das demonstrações financeiras.
- **Reflete as atividades da organização:** relatórios externos refletem as transações e eventos subjacentes para mostrar características e afirmações qualitativas.

6.3. Objetivos de relatórios internos

- **Refletir as escolhas da administração:** os relatórios internos fornecem à administração informações precisas e completas sobre as escolhas de gerenciamento e as informações necessárias para administrar a organização.

- **Considere o nível exigido de precisão:** a administração reflete o nível exigido de precisão e exatidão adequado às necessidades do usuário em objetivos de relatórios não financeiros e materialidade dentro dos objetivos de relatórios financeiros.

- **Refletem as atividades da organização**: os relatórios internos refletem as transações e eventos subjacentes dentro de uma faixa de limites aceitáveis.

6.4. Objetivos de Compliance

- **Reflitam leis e regulamentos externos:** leis e regulamentos estabelecem padrões mínimos de conduta que a organização integra aos objetivos de Compliance.

- **Considerar a tolerância ao risco:** a administração considera os níveis aceitáveis de variação em relação ao alcance dos objetivos de Compliance.

7. A organização identifica os riscos para a consecução de seus objetivos em toda a entidade e analisa os riscos como base para determinar como os riscos devem ser gerenciados.

- **7.1. Inclui organização e estruturas principais**. A organização identifica e avalia os riscos nos níveis da organização, região e divisão relevantes para o alcance dos objetivos.

- **7.2. Analisa fatores internos e externos.** A identificação de riscos considera fatores internos e externos e seu impacto na consecução dos objetivos.

- **7.3. Envolve níveis apropriados de gestão.** A organização implementa mecanismos eficazes de avaliação de riscos que envolvem níveis apropriados de gestão.

- **7.4. Estima a significância dos riscos identificados.** Os riscos identificados são analisados por meio de um processo que inclui a estimativa do potencial significância do risco.

- **7.5. Determina como responder aos riscos**. A avaliação de risco inclui considerar como o risco deve ser gerenciado e se deve aceitar, evitar, reduzir ou compartilhar o risco.

8. A organização considera o potencial de fraude na avaliação de riscos para o realização de objetivos.

- **8.1. Considera vários tipos de fraude**. A avaliação de fraude considera relatórios fraudulentos, possível perda de ativos e corrupção resultante das várias formas pelas quais a fraude e a má conduta podem ocorrer.

- **8.2. Avalia incentivos e pressões**. A avaliação do risco de fraude considera incentivos e pressões.

- **8.3. Avalia oportunidades.** A avaliação do risco de fraude considera oportunidades de aquisição, uso ou alienação não autorizada de ativos, alteração dos registros de relatórios da organização ou outros atos inapropriados.

- **8.4. Avalia atitudes e racionalizações**. A avaliação do risco de fraude considera como a administração e outros colaboradores podem se envolver ou justificar ações inadequadas.

9. A organização identifica e avalia mudanças que possam impactar significativamente o sistema de controle interno.

- **9.1. Avalia mudanças no ambiente externo.** O processo de identificação de riscos considera mudanças no ambiente regulatório, econômico e físico em que a organização opera.

- **9.2. Avalia mudanças no modelo de negócios.** A organização considera os impactos potenciais de novas linhas de negócios, composições dramaticamente alteradas de linhas de negócios existentes e operações comerciais adquiridas ou alienadas no sistema de controle interno, crescimento rápido, dependência variável de geografias estrangeiras e novas tecnologias.

- **9.3. Avalia mudanças na liderança.** A organização considera mudanças na gestão e respectivas atitudes em filosofias sobre o sistema de controle interno.

Atividades de controle

10. A organização seleciona e desenvolve atividades de controle que contribuem para a mitigação dos riscos ao alcance dos objetivos em níveis aceitáveis.

- **10.1. Integra-se com a avaliação de risco.** As atividades de controle ajudam a garantir que as respostas aos riscos que abordam e mitigam os riscos sejam realizadas.

- **10.2. Considera fatores específicos da organização.** A administração considera como o ambiente, a complexidade, a natureza e o escopo de suas operações, bem como as características específicas da organização, afetam a seleção e o desenvolvimento das atividades de controle.

- **10.3. Determina os processos de negócios relevantes.** A administração determina quais processos de negócios relevantes requerem atividades de controle.

- **10.4. Avalia uma combinação de tipos de atividades de controle.** As atividades de controle incluem uma gama e variedade de controles e podem incluir um equilíbrio de abordagens para mitigar os riscos, considerando tanto os controles manuais e automatizados quanto os controles preventivos e de detecção.

- **10.5. Considera em que nível as atividades são aplicadas.** A administração considera as atividades de controle em vários níveis da organização.

- **10.6. Aborda a segregação de funções.** A administração segrega funções incompatíveis e, quando tal segregação não é prática, a administração seleciona e desenvolve atividades alternativas de controle.

11. A organização seleciona e desenvolve atividades gerais de controle sobre a tecnologia para apoiar o alcance dos objetivos.

- **11.1. Determina a dependência entre o uso de tecnologia em processos de negócios e controles gerais de tecnologia.** A administração entende e determina a dependência e a ligação entre processos de negócios, atividades de controle automatizado e controles gerais de tecnologia.

- **11.2. Estabelece atividades relevantes de controle de infraestrutura de tecnologia.** A administração seleciona e desenvolve atividades de controle sobre a infraestrutura de tecnologia, que são projetadas e implementadas para garantir integridade, precisão e disponibilidade do processamento de tecnologia.

- **11.3. Estabelece atividades relevantes de controle do processo de gerenciamento de segurança.** A administração seleciona e desenvolve atividades de controle que são projetadas e implementadas para restringir os direitos de acesso à tecnologia a usuários autorizados de acordo com suas responsabilidades de trabalho e para proteger os ativos da organização contra ameaças externas.

- **11.4. Estabelece atividades relevantes de controle de processo de aquisição, desenvolvimento e manutenção de tecnologia.** A administração seleciona e desenvolve atividades de controle sobre a aquisição, desenvolvimento e manutenção de tecnologia e sua infraestrutura para atingir os objetivos da administração.

12. A organização desenvolve atividades de controle por meio de políticas que estabelecem o que é esperado e procedimentos que colocam as políticas em prática.

- **12.1. Estabelece políticas e procedimentos para apoiar a implantação das diretrizes da administração.** A administração estabelece atividades de controle que são incorporadas aos procedimentos de negócios e às atividades diárias dos colaboradores por meio de políticas.

- **12.2. Estabelece responsabilidade e responsabilidade pela execução de políticas e procedimentos**. A administração estabelece a responsabilidade e prestação de contas pelas atividades de controle com a administração (ou outro pessoal designado) da unidade de negócios ou função na qual residem os riscos relevantes.

- **12.3. Executa em tempo hábil.** O pessoal responsável realiza atividades de controle em tempo hábil, conforme definido pelas políticas e procedimentos.

- **12.4. Toma ação corretiva.** O pessoal responsável investiga e atua em questões identificadas como resultado da execução de atividades de controle.

- **12.5. Realiza usando pessoal competente.** Pessoal competente com autoridade suficiente realiza atividades de controle com diligência e foco contínuo.

- **12.6. Reavalia políticas e procedimentos.** A administração revisa periodicamente as atividades de controle para determinar sua relevância contínua e as atualiza quando necessário.

Informação e Comunicação

13. A organização obtém ou gera e usa informações relevantes e de qualidade para apoiar o funcionamento do controle interno.

- **13.1. Identifica os requisitos de informação.** Existe um processo para identificar as informações necessárias e esperadas para apoiar o funcionamento de outros componentes do controle interno e a consecução dos objetivos da organização.

- **13.2. Captura fontes internas e externas de dados.** Os sistemas de informação capturam fontes internas e externas de dados.

- **13.3. Processa dados relevantes em informações.** Os sistemas de informação processam e transformam dados relevantes em informações.

- **13.4. Mantém a qualidade durante todo o processamento.** Os sistemas de informação produzem informações oportunas, atuais, precisas, completas, acessíveis, protegidas, verificáveis e retidas. As informações são revisadas para avaliar sua relevância no suporte aos componentes de controle interno.

- **13.5. Considera custos e benefícios.** A natureza, a quantidade e a precisão das informações comunicadas são proporcionais e apoiam a realização dos objetivos.

14. A organização comunica internamente informações, incluindo objetivos e responsabilidades de controle interno, necessárias para apoiar o funcionamento do controle interno.

- **14.1. Comunica informações de controle interno.** Existe um processo para comunicar as informações necessárias para permitir que todo o pessoal entenda e execute suas responsabilidades de controle interno.

- **14.2. Comunica-se com as entidades reguladoras.** Existe comunicação entre a administração e as entidades reguladoras para que ambos tenham as informações necessárias para cumprir seus papéis em relação aos objetivos da organização.

- **14.3. Fornece linhas de comunicação separadas.** Canais de comunicação separados, como linhas diretas de denunciantes, estão em vigor e servem como um mecanismo à prova de falhas para permitir comunicação anônima e confidencial quando os canais normais estão inoperantes ou ineficazes.

- **14.4. Seleciona métodos relevantes de comunicação.** O método de comunicação considera o momento, o público e a natureza da informação.

15. A organização se comunica com partes externas sobre assuntos que afetam o funcionamento do controle interno.

- **15.1. Comunica-se com partes externas.** Existem processos para comunicar informações relevantes e oportunas a partes externas, incluindo parlamento, parceiros, reguladores e outras partes externas.

- **15.2. Permite comunicações de entrada.** Os canais de comunicação abertos permitem a entrada de beneficiários ou clientes, fornecedores, auditores externos, reguladores e outros, fornecendo informações relevantes aos órgãos de administração e governança.

- **15.3. Comunica-se com entidades reguladoras.** A informação relevante resultante das avaliações realizadas por entidades externas é comunicada às entidades reguladoras.

- **15.4. Fornece linhas de comunicação separadas.** Canais de comunicação separados, como linhas diretas de denunciantes, estão em vigor e servem como mecanismos à prova de falhas para permitir comunicação anônima ou confidencial quando os canais normais estão inoperantes ou ineficazes.

- **15.5. Seleciona métodos relevantes de comunicação.** O método de comunicação considera o tempo, o público e a natureza da comunicação e os requisitos e expectativas legais, regulatórios e fiduciários.

Atividades de Monitoramento

16. A organização seleciona, desenvolve e realiza avaliações contínuas e/ou separadas para verificar se os componentes do controle interno estão presentes e funcionando.

- **16.1. Considera uma mistura de avaliações contínuas e separadas.** A gestão inclui um balanço de avaliações contínuas e separadas.
- **16.2. Considera a taxa de variação.** A administração considera a taxa de mudança nos negócios e processos de negócios ao selecionar e desenvolver avaliações contínuas e separadas.
- **16.3. Estabelece entendimentos básicos.** O design e o estado atual de um sistema de controle interno são usados para estabelecer uma linha de base para avaliações contínuas e separadas.
- **16.4. Usa pessoal experiente.** Os avaliadores que realizam avaliações contínuas e separadas possuem conhecimento suficiente para entender o que está sendo avaliado.
- **16.5. Integra-se com os processos de negócios.** As avaliações contínuas são incorporadas ao processo de negócios e se ajustam às mudanças nas condições.
- **16.6. Ajusta escopo e frequência.** A administração varia o escopo e a frequência de avaliações separadas, dependendo do risco.
- **16.7. Avalia objetivamente.** Avaliações separadas são realizadas periodicamente para fornecer feedback objetivo.

17. A organização avalia e comunica tempestivamente as deficiências dos controles internos às partes responsáveis pela adoção de ações corretivas, incluindo a alta administração e os entidades reguladoras, conforme o caso.

- **17.1. Avalia resultados.** A administração e o conselho, conforme apropriado, avaliam os resultados das avaliações contínuas e separadas.
- **17.2. Comunica deficiências.** As deficiências são comunicadas às partes responsáveis pela tomada de ações corretivas e à alta administração e ao conselho, conforme apropriado.
- **17.3. Monitora as ações corretivas.** A administração rastreia se as deficiências são corrigidas em tempo hábil.

ANEXO B1. O AMBIENTE DE CONTROLE

Os anexos a seguir devem ajudar os auditores internos a interpretar e aplicar os cinco componentes e os 17 princípios de controle interno. Cada anexo se concentra em um dos componentes, ilustrando como os pontos de foco podem ser interpretados, delineando o objetivo e as principais características de cada princípio e fornecendo um conjunto de critérios para avaliar a eficácia do controle interno.

Este anexo enfoca o Componente 1 - O Ambiente de Controle, que é a base de todos os outros componentes do controle interno. O ambiente de controle reflete o tom no topo de uma organização. Depende em parte das estruturas estabelecidas pela gestão, mas também da forma como as pessoas agem dentro da organização no cumprimento das suas responsabilidades. Por exemplo, há necessidade de políticas que expliquem como as pessoas devem agir em determinadas situações, mas também é preciso que a gestão demonstre por meio de suas ações que está seguindo essa orientação.

O COSO identifica **cinco princípios dentro desse componente**, listados na tabela abaixo.

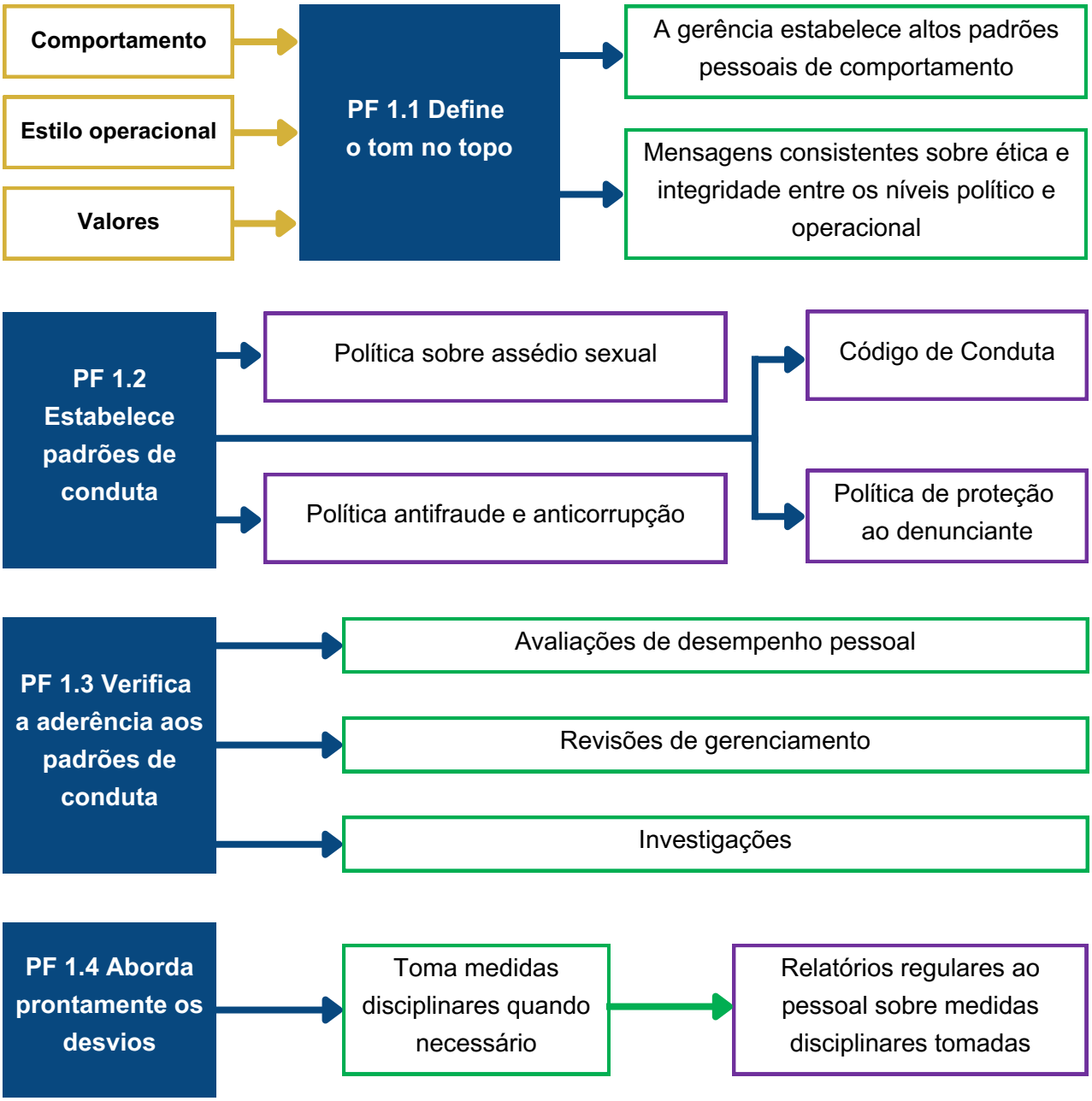
Tabela 2. Os Princípios e Pontos de Foco do Componente 1 – O Ambiente de Controle

Princípio	Pontos de Foco (PF)
1 A organização demonstra um compromisso com a integridade e os valores éticos.	1.1. Define o tom no topo.
	1.2. Estabelece padrões de conduta.
	1.3. Verifica o cumprimento das normas de conduta.
	1.4. Aborda os desvios prontamente.

Princípio	Pontos de Foco (PF)
2 O conselho demonstra independência da administração e supervisiona o desenvolvimento e o desempenho do controle interno.	2.1. Estabelece responsabilidades de supervisão.
	2.2. Tem acesso a habilidades relevantes.
	2.3. Opera de forma independente.
	2.4. Fornece supervisão do sistema de controle interno.
3 A administração, com a supervisão do conselho, estabelece estruturas, linhas de subordinação e autoridades e responsabilidades apropriadas na busca dos objetivos.	3.1. Considera todas as estruturas da organização.
	3.2. Estabelece linhas de reporte.
	3.3. Define, atribui e limita autoridades e responsabilidades.
4 A organização demonstra um compromisso para atrair, desenvolver e reter indivíduos competentes em alinhamento com os objetivos.	4.1. Estabelece políticas e procedimentos.
	4.2. Avalia a competência e aborda as deficiências.
	4.3. Atrai, desenvolve e retém indivíduos.
	4.4. Planeja e se prepara para a sucessão.
5 A organização responsabiliza os indivíduos por suas responsabilidades de controles internos na busca dos objetivos.	5.1. Impõe a prestação de contas por meio de estruturas, autoridades e responsabilidades.
	5.2. Estabelece medidas de desempenho, incentivos e recompensas.
	5.3. Avalia medidas de desempenho, incentivos e recompensas por relevância contínua.
	5.4. Considera pressões excessivas.
	5.5. Avalia o desempenho e recompensa ou disciplina os indivíduos.

Princípio 1. A organização demonstra um compromisso com a integridade e os valores éticos

Figura 4. Interpretação do Princípio 1



Comentário

Não é possível que as pessoas ajam com integridade se não estiverem cientes dos padrões éticos que se espera que sigam. É crucial, portanto, que cada organização fornece ao seu pessoal orientações que explicam os padrões esperados.

Isso deve incluir disposições para proteger os indivíduos que denunciam irregularidades (conhecidos como denunciantes). Tendo estabelecido padrões claros de comportamento, é essencial que o comportamento real seja revisado e que quaisquer desvios sejam totalmente investigados com ação disciplinar quando necessário. No setor público há também a necessidade de mensagens consistentes sobre a importância da ética e da integridade entre os níveis político e operacional. Tanto os políticos quanto os servidores públicos devem demonstrar ética e integridade.

Critérios para avaliar a eficácia do controle interno

Os gestores seniores "fazem o que falam", onde o que eles dizem em termos de comportamento que esperam dos colaboradores é consistente com a maneira como agem?

A organização tem uma ou mais políticas que definem padrões de comportamento esperados para gestores e colaboradores, incluindo declarações sobre ética e valores? Elas incluem:

- Código de Ética.
- Política antifraude e anticorrupção.
- Política sobre assédio e abuso sexual.
- Arranjos para proteger os denunciantes.
- Treinamento nos padrões de comportamento esperados.
- Lembretes regulares aos colaboradores sobre a necessidade de desempenhar suas funções com integridade de forma que atendam aos padrões éticos estabelecidos.

Existem processos em vigor para avaliar o desempenho dos indivíduos e equipes no cumprimento dos padrões éticos esperados? Por exemplo:

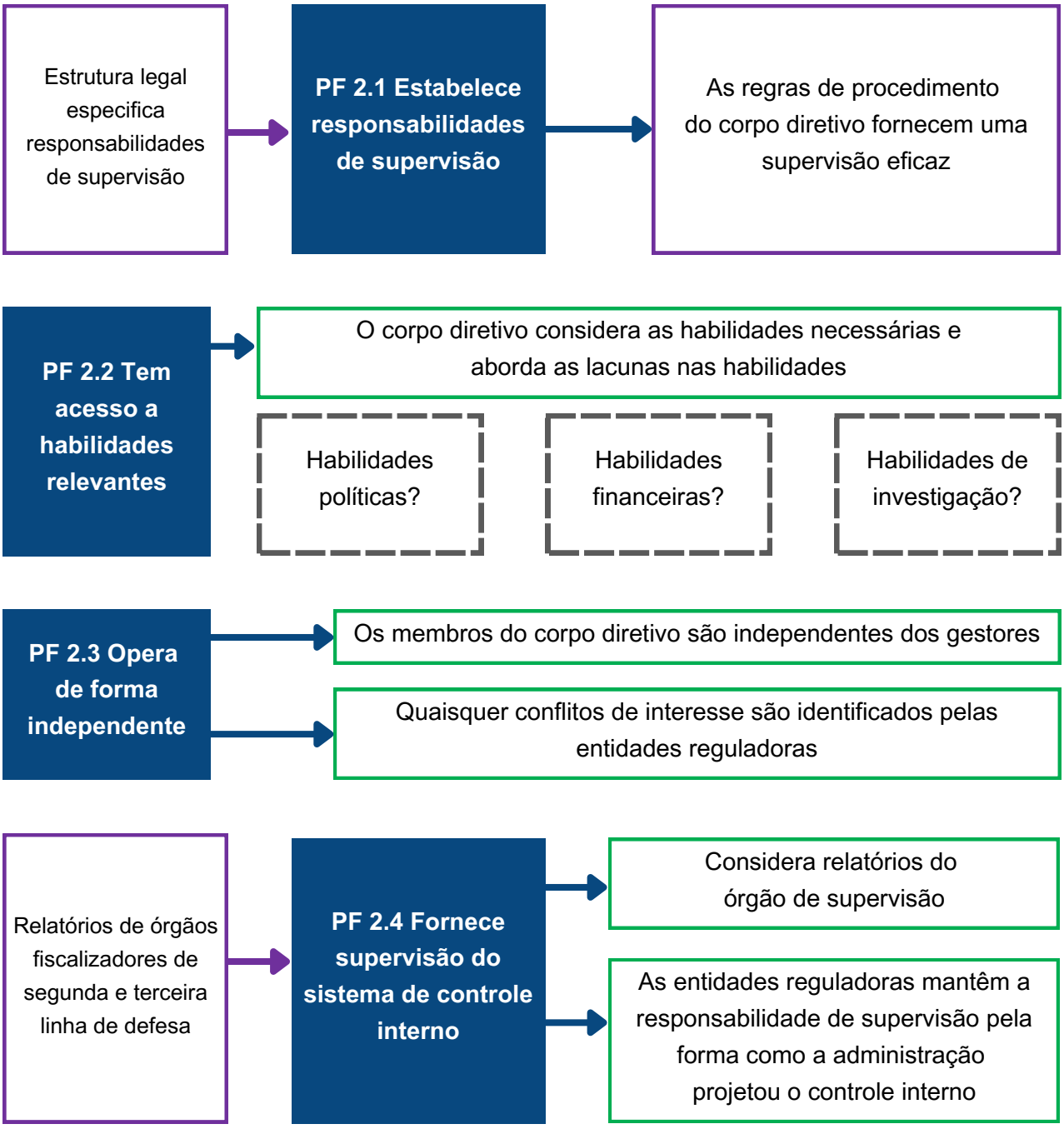
- Todos os colaboradores devem se autoavaliar e declarar regularmente se eles atenderam aos padrões de comportamento esperados.
- Os conflitos de interesse no setor público são claramente definidos, declarados, regularmente registrados / assinados e monitorados.
- As declarações de bens e despesas são feitas regularmente.

Existe um processo claro para gerenciar desvios dos padrões esperados? Por exemplo:

- Os dados são mantidos em todos os desvios dos padrões esperados.
- Os desvios dos padrões esperados são investigados e ações são tomadas para corrigir as deficiências.

Princípio 2. Órgãos governamentais demonstram independência da administração e exercem supervisão do desenvolvimento e desempenho do controle interno

Figura 5. Interpretação do Princípio 2



Comentário

Este princípio foi modificado a partir da orientação COSO que se refere a um conselho de administração. O princípio se aplica a organizações do setor público mesmo quando não há um conselho de administração com responsabilidades de supervisão. Isso ocorre porque todas as organizações do setor público devem estar sujeitas a algum grau de supervisão de órgãos de supervisão externos à entidade. Há uma variedade de opções de supervisão no setor público, conforme observado na Tabela 3 abaixo.

Tabela 3. Possíveis entidades reguladoras no setor público

Arranjos no setor público para cumprir o papel de órgão governamental como identificados durante as discussões da PEMPAL
1. Chefe da organização (ministro, etc.) - uma única pessoa
2. Comitê de supervisão externa que pode assumir diferentes formas (por exemplo, comitê parlamentar, comitê governamental, comitê representado por diferentes ministérios)
3. Supervisão pelo ministério de linha ou uma organização superior
4. Dupla liderança: ministro (líder político) mais secretário-geral (líder administrativo)
5. Diretoria da agência/departamento representada apenas pelo executivo (com os indicados dentro da organização)
6. Comitês de auditoria no nível de agência/departamento com diretores não executivos / membros independentes
7. Comitê de auditoria centralizado para o governo
8. Painéis temáticos: por ex. conselho de controle interno liderado por um secretário-geral (ou adjunto)
9. Unidade ou pessoa dedicada na administração presidencial (quando relevante) com responsabilidades específicas de supervisão

No setor público, os arranjos de supervisão geralmente são identificados em legislação e pode ser complementado por regras de procedimento para certas entidades reguladoras. As principais características do COSO são que as entidades reguladoras devem operar de forma independente e ter as habilidades para trabalhar de forma eficaz. Também é essencial que as entidades reguladoras realmente revisem a operação dos controles internos. Muitas vezes, isso pode ser feito revisando os relatórios gerados na segunda e na terceira linhas.

Critérios para avaliar a eficácia do controle interno

Existe um órgão governamental independente responsável pela supervisão da administração?

Se não, que nível de supervisão independente existe das ações da administração? Consulte a Tabela 3 acima para exemplos do tipo de acordos de supervisão que podem existir nos países PEMPAL.

Os arranjos de supervisão estão claramente definidos, por exemplo:

- Uma estrutura legal que defina a responsabilidade de supervisão sobre o controle interno.

O corpo diretivo tem experiência para supervisionar o trabalho da organização? Por exemplo:

- As competências necessárias e as experiências relevantes são definidas e correspondem aos objetivos da organização.
- O corpo diretivo é composto por membros com várias habilidades e competências apropriadas (educação e qualificação).
- Existe um processo claro para nomear ou recrutar membros do corpo diretivo.
- O corpo diretivo tem acesso a especialistas independentes conforme necessário.
- O corpo diretivo apoia comprovadamente a independência da auditoria interna como terceira linha de defesa.

O corpo diretivo opera independentemente da administração? Por exemplo:

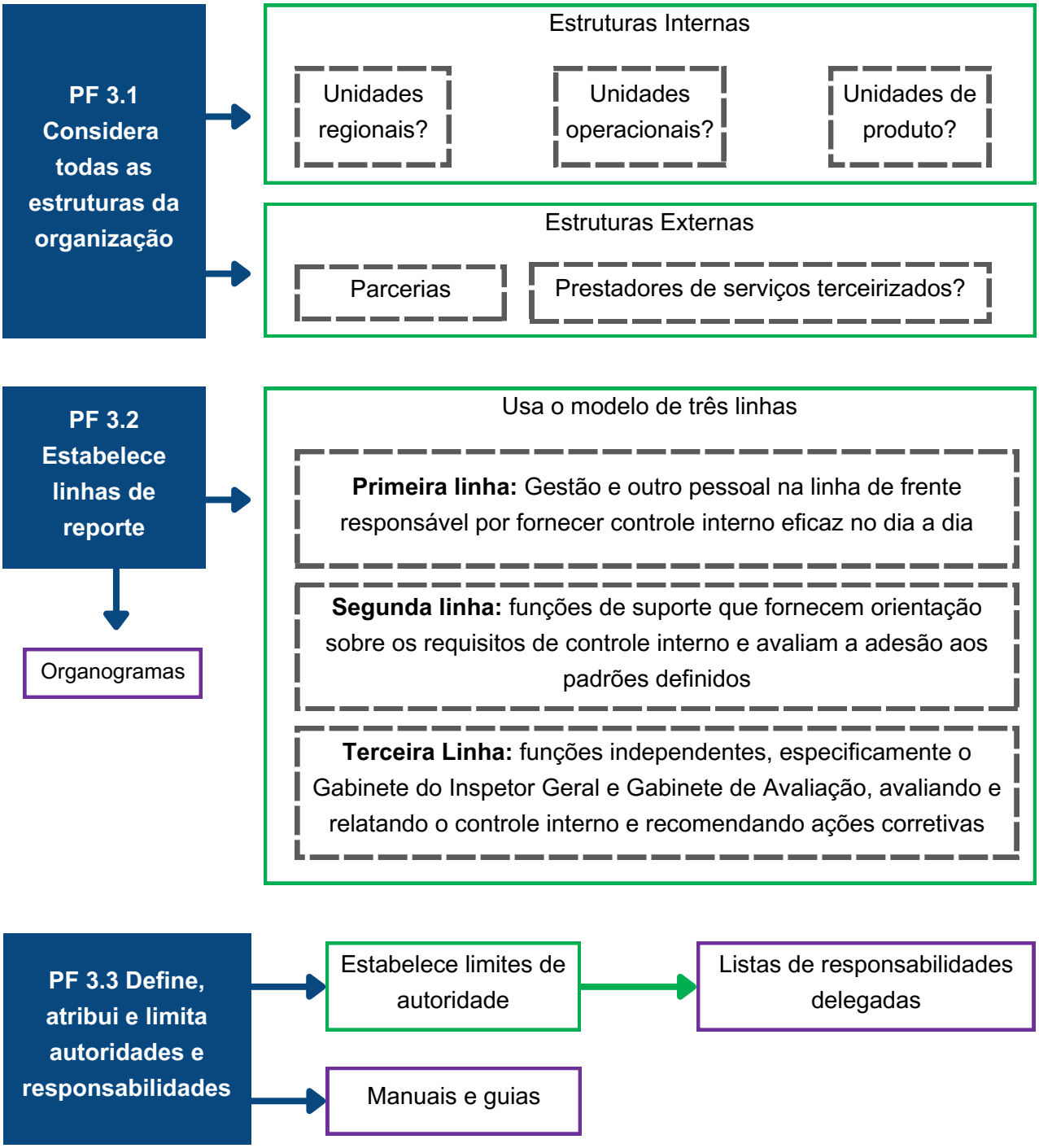
- Há uma clara separação entre o papel de tomada de decisão gerencial e o função de supervisão/consultoria.
- Existe um mandato claro para a supervisão do controle interno.
- As informações necessárias para o exercício da supervisão são coletadas no prazo e relatadas de maneira precisa e confiável.
- Os arranjos de supervisão foram avaliados quanto à eficiência e eficácia pela instituição suprema de auditoria (SAI).

O corpo diretivo supervisiona a implementação do sistema de controle interno pela administração? Por exemplo:

- Existe um sistema estabelecido de supervisão de controle interno.
- Existem critérios independentes para relatar questões de controle interno ao corpo governante.
- Existe um sistema estabelecido para fornecer uma declaração sobre controlar o status do sistema dentro da organização.
- Existe uma opinião anual da auditoria interna sobre a eficácia do controle interno na organização.
- O comitê de auditoria fornece um relatório público sobre a eficácia do controle interno.

Princípio 3. A administração, com a supervisão do corpo diretivo, estabelece estruturas, linhas de subordinação e autoridades e responsabilidades apropriadas na busca dos objetivos

Figura 6. Interpretação do Princípio 3



Comentário

A forma como uma organização está estruturada tem um impacto direto na forma como o controle interno opera. Por exemplo, organizações com escritórios regionais separados operarão de forma diferente daquelas com um escritório central. As estruturas desejadas precisam ser complementadas com linhas hierárquicas claras e estas devem ser refletidas nos organogramas oficiais. Deve haver uma definição clara da autoridade e responsabilidade de todos os indivíduos da organização. Estes devem ser claramente definidos em manuais e guias. Muitas organizações também têm listas separadas de todas as autoridades delegadas.

A melhor prática atual é usar o “modelo de três linhas” como um modelo organizacional interno. Estes diferenciam entre (a) a responsabilidade de primeira linha dos gestores e do pessoal para fornecer controle interno eficaz no dia a dia; (b) as funções de suporte de segunda linha que fornecem orientação sobre atividades de risco, controle e conformidade e revisam a adesão a tal orientação; e (c) funções independentes, como auditoria interna, que fornecem uma terceira linha de defesa, avaliando e relatando a eficácia do controle interno.

Critérios para avaliar a eficácia do controle interno

A administração estabeleceu estruturas internas claras, incluindo conforme necessário para unidades subsidiárias, como escritórios regionais? Por exemplo:

- Existe uma estrutura organizacional aprovada.
- A estrutura estabelecida é clara e de fácil compreensão.
- As relações com os parceiros externos são claramente definidas pela gestão.
- Existem contratos para prestadores de serviços terceirizados que especificam claramente as responsabilidades desses prestadores em relação ao controle interno.
- Órgãos de governo revisam regularmente a eficácia da organização estrutura.

Os limites de autoridade são claramente definidos e comunicados ao pessoal? Por exemplo:

- Existe uma declaração clara por escrito das autoridades delegadas de todos os colaboradores.
- Os colaboradores recebem manuais ou outras orientações onde os limites de autoridade são definidas.
- A auditoria interna fornece garantia sobre a clareza das autoridades e responsabilidades.

As estruturas internas resultam em linhas hierárquicas claras? Por exemplo:

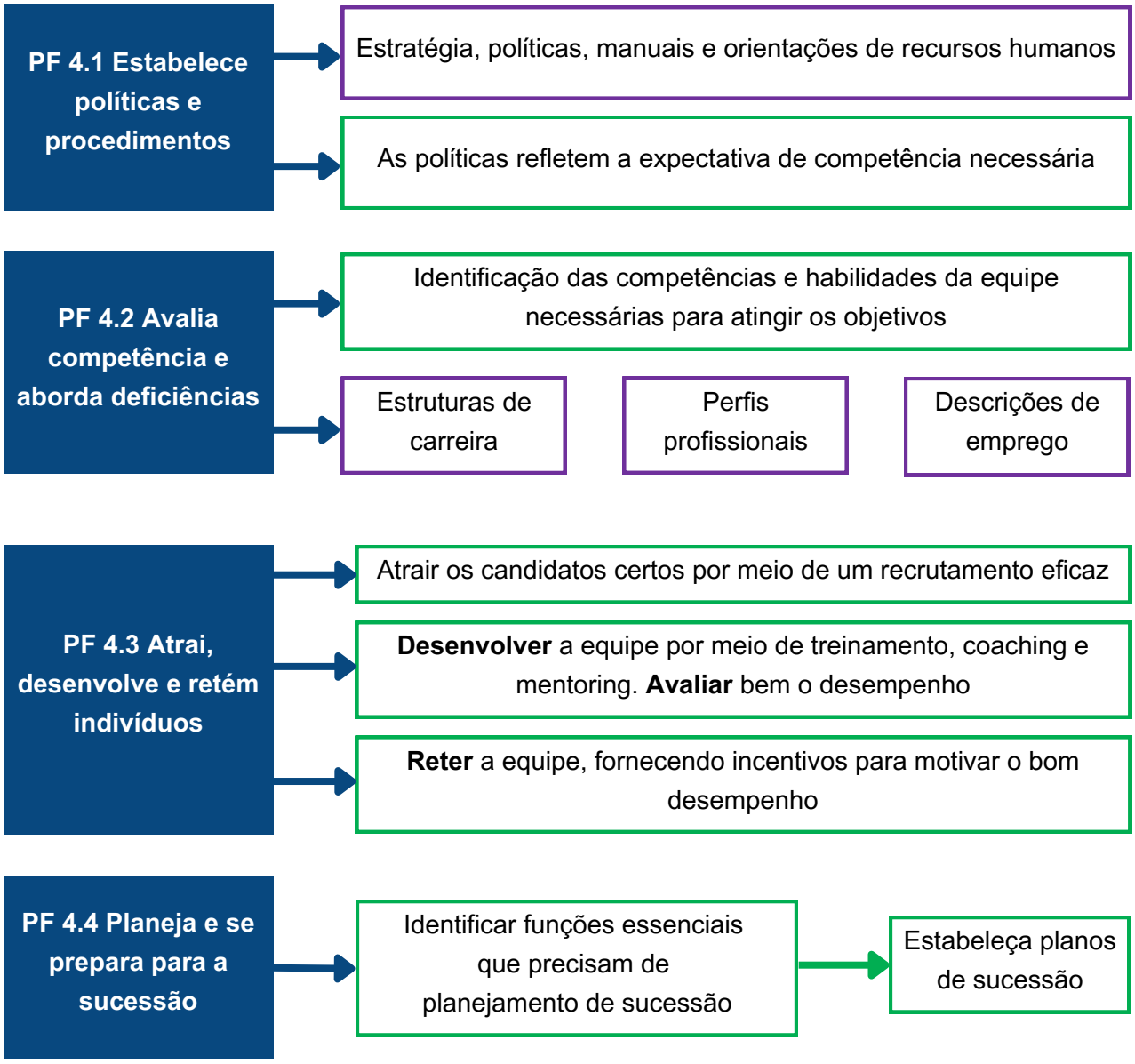
- Existem organogramas formais que especificam as linhas hierárquicas.
- Poucos indivíduos têm responsabilidades duplas de relatórios.

A organização entende e usa o conceito de três linhas para manter um controle interno eficaz? Por exemplo:

- Todos os colaboradores estão cientes das funções da primeira, segunda e terceira linhas.
- Os resultados da terceira linha de defesa são utilizáveis e acionáveis.

Princípio 4. A organização demonstra um compromisso para atrair, desenvolver e reter indivíduos competentes em alinhamento com os objetivos

Figura 7. Interpretação do Princípio 4



Comentário

Você precisa de boas pessoas para implementar controles internos de forma eficaz. Este princípio examina se existem políticas de recursos humanos que reflitam a necessidade de pessoal competente, incluindo sistemas para avaliar se o pessoal desempenha suas funções de forma eficaz.

Organizações com alta rotatividade de pessoal ou que não conseguem atrair e reter colaboradores do calibre certo terão dificuldade em administrar sistemas de controle interno eficazes. O princípio, portanto, analisa a capacidade da organização de atrair, desenvolver e reter pessoas. Também é importante se preparar para a sucessão de pessoas em cargos importantes.

Critérios para avaliar a eficácia do controle interno

Existe uma declaração clara das políticas e práticas de recursos humanos da organização? Por exemplo:

- Um documento de estratégia de recursos humanos descreve os objetivos das políticas de recursos humanos da organização.
- Circulares, manuais e guias identificam claramente as competências e habilidades necessárias para o pessoal, usando conforme necessário estruturas de carreira, declarações de competência, descrições de cargos etc.
- A estratégia e as políticas de recursos humanos são revisadas periodicamente pelas entidades reguladoras.

A organização avalia a competência do pessoal e aborda as deficiências? Por exemplo:

- Existe um sistema formal de avaliação de desempenho aplicado a todos os colaboradores.
- O desempenho do pessoal é regularmente avaliado em relação aos padrões de competência esperados.
- Existem testes formais exigidos das habilidades da equipe em funções críticas, como auditoria interna.

A organização pode atrair, desenvolver e reter pessoal de qualidade suficiente para desempenhar suas funções? Por exemplo:

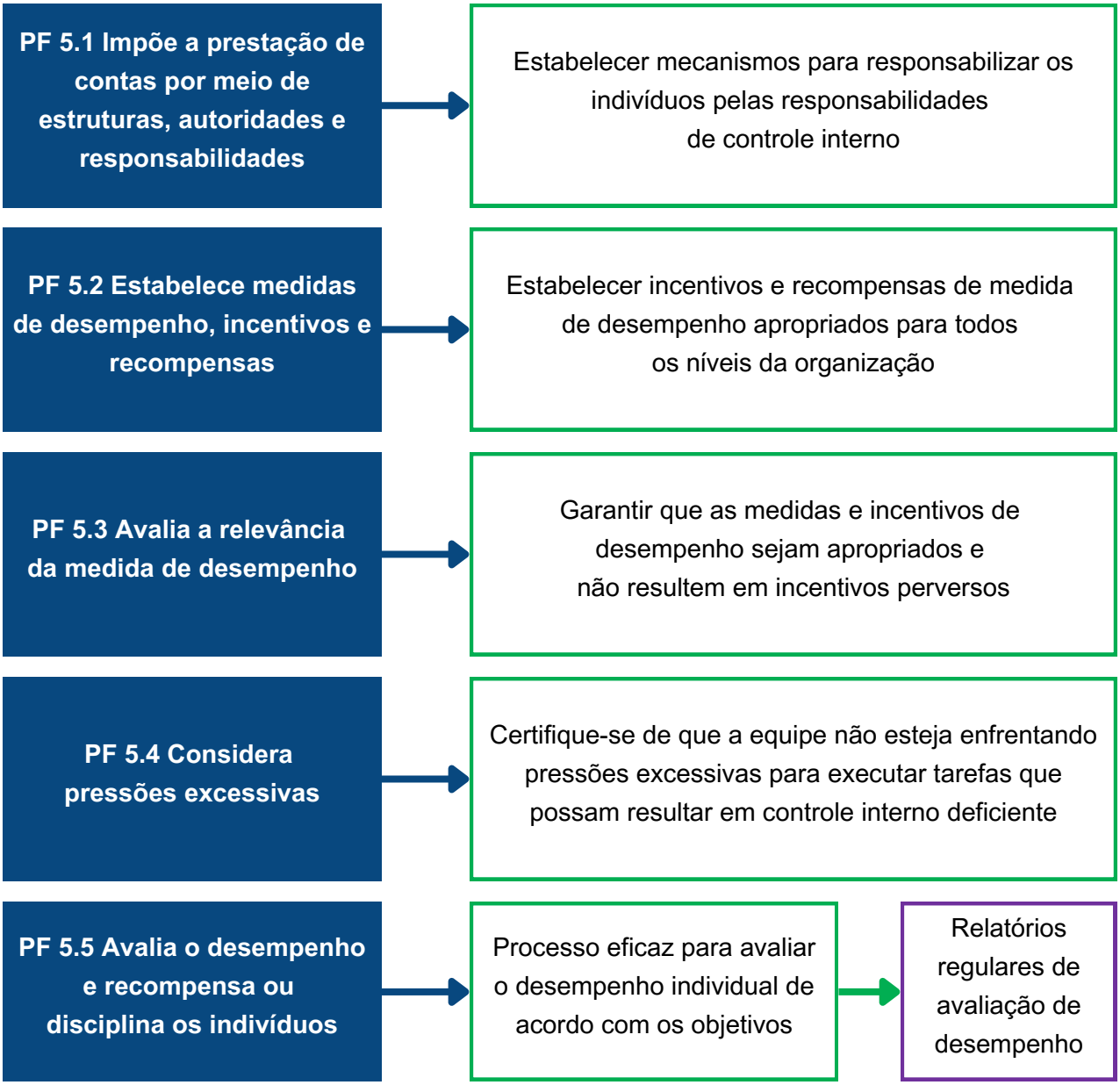
- Existe um mecanismo de recrutamento com regras pré-definidas e claras.
- Há qualificações claras exigidas para todos os colaboradores no momento do recrutamento.
- Existe um plano de treinamento para a organização como um todo e pessoal planos de desenvolvimento para indivíduos.
- A organização fornece suporte de orientação para desenvolver o pessoal.
- Existe um mecanismo para enviar pessoal para seminários, conferências e workshops internacionais como a PEMPAL.
- Os requisitos de promoção dentro da organização estão relacionados a habilidades adicionais necessárias em níveis mais altos da organização.
- Existem mecanismos para recompensar altos níveis de desempenho do pessoal com recompensas financeiras e não financeiras.

A organização planeja e se prepara para a sucessão? Por exemplo:

- A organização identificou cargos-chave que não devem ser deixados sem preenchimento.
- A organização identificou cargos onde a rotatividade de colaboradores é esperada.
- Existe um “plano de sucessão” para preenchimento de cargos-chave na organização.
- Existe uma política de rotação regular do pessoal para alargar a combinação de competências disponíveis.
- Existe um programa de orientação para ajudar a identificar futuros líderes.

Princípio 5. A organização responsabiliza os indivíduos por suas responsabilidades de controle interno na busca dos objetivos

Figura 8. Interpretação do Princípio 5



Comentário

O controle interno não será eficaz se não houver processos em vigor para responsabilizar os indivíduos pela implementação do controle interno.

A responsabilidade é reforçada por um sistema de gerenciamento de desempenho eficaz para indivíduos que recompensa ou disciplina indivíduos. Os sistemas de gestão de desempenho devem considerar quaisquer pressões excessivas que possam influenciar a maneira como as pessoas executam suas funções.

Critérios para avaliar a eficácia do controle interno

A organização reforça a prestação de contas por meio de estruturas, autoridades e responsabilidades? Por exemplo:

- As responsabilidades são identificadas e atribuídas aos indivíduos.
- Existe um sistema de avaliação de desempenho que atua em diferentes níveis da organização e foca em como os gestores gerenciam sua região / escritórios / divisões / unidades.
- Os colaboradores estão cientes de suas responsabilidades por meio de descrições de cargos ou outros mecanismos.
- As responsabilidades atendem ao controle interno e aos objetivos de negócios da organização.
- Existem cadeias de responsabilidade bem compreendidas e a maioria dos colaboradores é responsabilizada por suas responsabilidades de controle interno.
- Os objetivos individuais estão ligados a objetivos de nível superior na estratégia ou plano de gestão.
- Todos os colaboradores são regularmente responsabilizados por suas responsabilidades de controle interno.

A organização estabeleceu incentivos e recompensas de medidas de desempenho em todos os níveis da organização? Por exemplo:

- Existe uma política de definição de objetivos e indicadores-chave de desempenho (KPIs). Em diferentes níveis de maturidade, isso pode existir nos níveis de “entidade”, “unidade de negócios” e “indivíduo”.
- Todos os colaboradores estão ativamente envolvidos na definição de seus objetivos de desempenho e KPIs relacionados.

A organização avalia a relevância de suas medidas de desempenho?

- A segunda linha de defesa é responsável por revisar a relevância das medidas de desempenho.
- A qualidade e relevância das medidas de desempenho são regularmente avaliadas pela auditoria interna.
- A administração atesta a relevância de suas medidas de desempenho.

A administração considera pressões excessivas que possam impactar a forma como as pessoas desempenham suas funções? Por exemplo:

- Existe um procedimento/mecanismo formalizado para medir a carga de trabalho do pessoal que identifica situações de sobrecarga ou subcarga e mecanismos para lidar com essas disparidades.
- A gerência identifica os colaboradores que não estão tirando folga suficiente de suas funções.
- Os colaboradores que sofrem de doenças relacionadas ao estresse são identificados e são feitas alterações nas cargas de trabalho para reduzir esse estresse.
- Existem acordos de aconselhamento do pessoal para identificar o pessoal que enfrenta pressões indevidas.

Existe uma política de gestão de desempenho do pessoal que preveja a avaliação regular do pessoal em termos de alcance dos seus objetivos? Por exemplo:

- Existe um sistema formal de avaliação de desempenho aplicado a todos os colaboradores.
- O sistema de avaliação resulta em relatórios formais de desempenho.
- Existe consistência entre o nível de funções assumidas e as recompensas.
- A avaliação de desempenho resulta na recompensa positiva e negativa (financeira e não financeira) do pessoal.

ANEXO B2. AVALIAÇÃO DE RISCO

Este anexo concentra-se no Componente 2 – Avaliação de Riscos, que permite a uma organização considerar até que ponto os eventos potenciais têm impacto na consecução dos objetivos. A avaliação de riscos procura abordar as principais questões enfrentadas por uma organização:

- Os gestores estão plenamente conscientes dos riscos que correm os seus colaboradores?
- Existem áreas em que os colaboradores devem assumir riscos que devem ser considerados e apoiados pela alta administração?
- Qual é o limite de risco a que a organização e os seus colaboradores devem estar sujeitos?
- A organização está aceitando riscos que podem e devem ser compartilhados com outros?
- A organização está implementando controles que têm pouco impacto sobre os riscos que enfrenta?
- Alguns riscos podem ser simplesmente aceitos em vez de controlados?
- Os riscos são registrados em registros de riscos e são mantidos atualizados?

O COSO identifica **quatro princípios dentro desse componente**, listados na tabela abaixo.

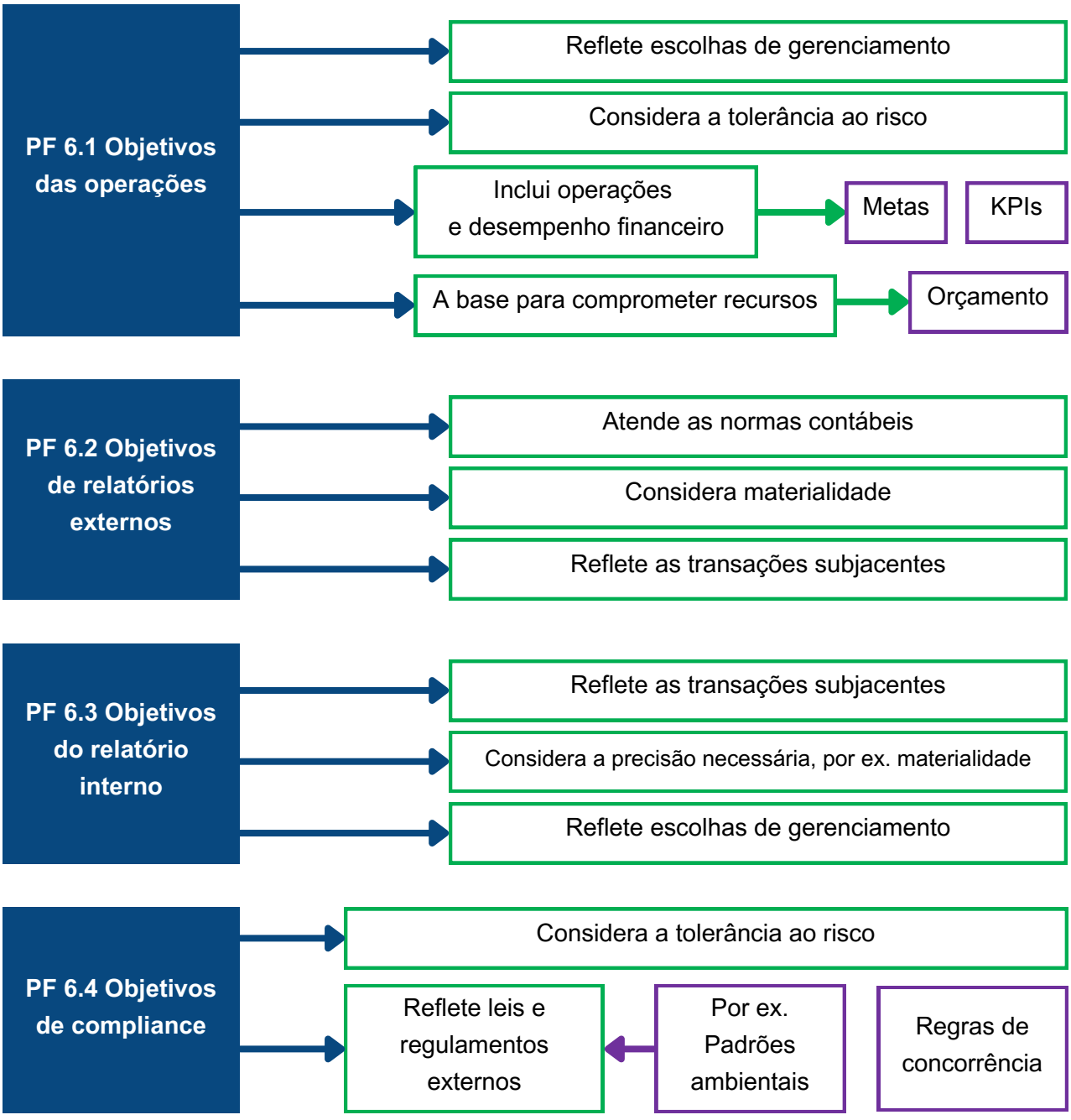
Tabela 4. Os Princípios e Focos do Componente 2 – Gestão de Riscos

Princípio	Pontos de Foco
6 A organização especifica os objetivos com clareza suficiente para permitir a identificação e avaliação dos riscos relativos aos objetivos.	6.1. Objetivos de operações
	6.2. Objetivos de relatórios externos
	6.3. Objetivos de relatórios internos
	6.4. Objetivos de compliance

Princípio	Pontos de Foco
7 A organização identifica os riscos para a consecução de seus objetivos em toda a entidade e analisa os riscos como base para determinar como os riscos devem ser gerenciados.	7.1. Inclui organização e estruturas principais.
	7.2. Analisa fatores internos e externos.
	7.3. Envolve níveis apropriados de gestão.
	7.4. Estima a significância dos riscos identificados.
	7.5. Determina como responder aos riscos.
8 A organização considera o potencial de fraude na avaliação de riscos para a realização de objetivos.	8.1. Considera vários tipos de fraude.
	8.2. Avalia incentivos e pressões.
	8.3. Avalia oportunidades.
	8.4. Avalia atitudes e racionalizações.
9 A organização identifica e avalia mudanças que possam impactar significativamente o sistema de controle interno.	9.1. Avalia mudanças no ambiente externo.
	9.2. Avalia mudanças no modelo de negócios.
	9.3. Avalia mudanças na liderança.

Princípio 6. A organização especifica os objetivos com clareza suficiente para permitir a identificação e avaliação dos riscos relacionados aos objetivos

Figura 9. Interpretação do Princípio 6



Comentário

A definição de objetivos é uma pré-condição tanto para a prestação de contas quanto para a realização de uma avaliação de risco eficaz. Os objetivos devem ser definidos antes que os gestores possam identificar e avaliar os riscos para sua realização e tomar as ações necessárias para gerenciar esses riscos. E nenhum sistema de prestação de contas pode funcionar sem a existência de objetivos claros. Todos os objetivos definidos devem ser “SMART”:

- Específicos
- Mensuráveis
- Cumpridos/Atingíveis
- Registrados e
- Programados

Este princípio estimula os gestores a se concentrarem nos quatro tipos de objetivos que podem existir no setor público.

Os **objetivos operacionais** se relacionam com o propósito de uma atividade ou programa do setor público e formam a base dos sistemas modernos de orçamento por programas. Os objetivos devem refletir as escolhas (dos gestores) sobre a melhor forma de implementar as políticas, pois sempre há opções relacionadas à implementação de políticas do setor público. Idealmente, os objetivos devem incluir metas e KPIs para promover a responsabilidade pela implementação. Os objetivos também devem refletir a tolerância ao risco. Uma forma de ilustrar a tolerância ao risco é que ela representa um nível abaixo de 100% de alcance dos objetivos que ainda seriam considerados um desempenho bem-sucedido. Por exemplo, a tolerância ao risco relacionada à segurança do público pode ser pequena, enquanto a tolerância ao risco para perdas de grãos armazenados nos estoques do governo pode ser alta porque há muitos fatores que podem levar a perdas de alimentos.

Os **objetivos de relatórios externos** referem-se à exigência imposta a todas as organizações do setor público de relatar seu desempenho a suas entidades reguladoras (geralmente o parlamento) e a seus stakeholders (que incluem o público em geral). Os relatórios externos devem refletir o conceito de materialidade, onde apenas os assuntos mais importantes são relatados. Eles também devem refletir a realidade mostrada nas transações subjacentes. Quaisquer relatórios financeiros devem ser produzidos de acordo com os padrões contábeis definidos.

Os **objetivos de relatórios internos** referem-se à ampla gama de relatórios internos dentro de uma organização que são críticos para a eficácia do controle interno. Assim como no relatório externo, os objetivos devem refletir a materialidade e as transações subjacentes. Os gestores também devem considerar a precisão dos relatórios internos. Preparar relatórios internos com um alto nível de precisão pode ser caro e não valer o esforço. Por exemplo, um relatório sobre a precisão do processamento de transações pode ser baseado em uma verificação de 100% de uma pequena amostra estatística de transações e ainda fornecer à administração informações confiáveis sobre o precisão do processamento da transação

Os **objetivos de compliance** referem-se às leis e requisitos externos que as organizações do setor público devem cumprir. Os objetivos de compliance podem, por exemplo, incluir leis sobre concorrência para contratos do setor público, tratamento de colaboradores e padrões ambientais.

Critérios para avaliar a eficácia do controle interno

A organização especifica objetivos relativos às suas operações? Por exemplo:

- Existe uma estratégia de alto nível para a organização que contém os objetivos do departamento como um todo.
- Os objetivos organizacionais refletem escolhas gerenciais e de nível político sobre a melhor forma de responder aos desafios políticos.
- A estratégia de alto nível é apoiada por metas e KPIs.
- Cada unidade de negócios da organização define objetivos anuais com metas e KPIs relacionados.
- Os objetivos operacionais formam a base para definir o orçamento da organização.
- Há uma declaração clara do apetite de risco geral da organização.
- Os níveis de tolerância ao risco são identificados para todos os objetivos principais e medidos por meio de KPIs relevantes.

A organização especifica os objetivos relativos aos relatórios externos? Por exemplo:

- A organização mantém registros de receitas e despesas em relação ao orçamento alocado e relata o resultado do orçamento ao ministério das finanças.
- A organização é obrigada a preparar demonstrações financeiras anuais de acordo com as normas contábeis adotadas para a organização como um todo.

- Existe um sistema de contabilidade automatizado que oferece suporte à preparação precisa de contas para refletir as transações subjacentes a um nível aceitável de materialidade.
- Relatórios de desempenho são fornecidos quando solicitados pelas entidades reguladoras.
- Existe um sistema para a preparação de relatórios anuais sobre o desempenho da organização em relação aos seus objetivos declarados.

A organização especifica os objetivos relativos aos relatórios internos? Por exemplo:

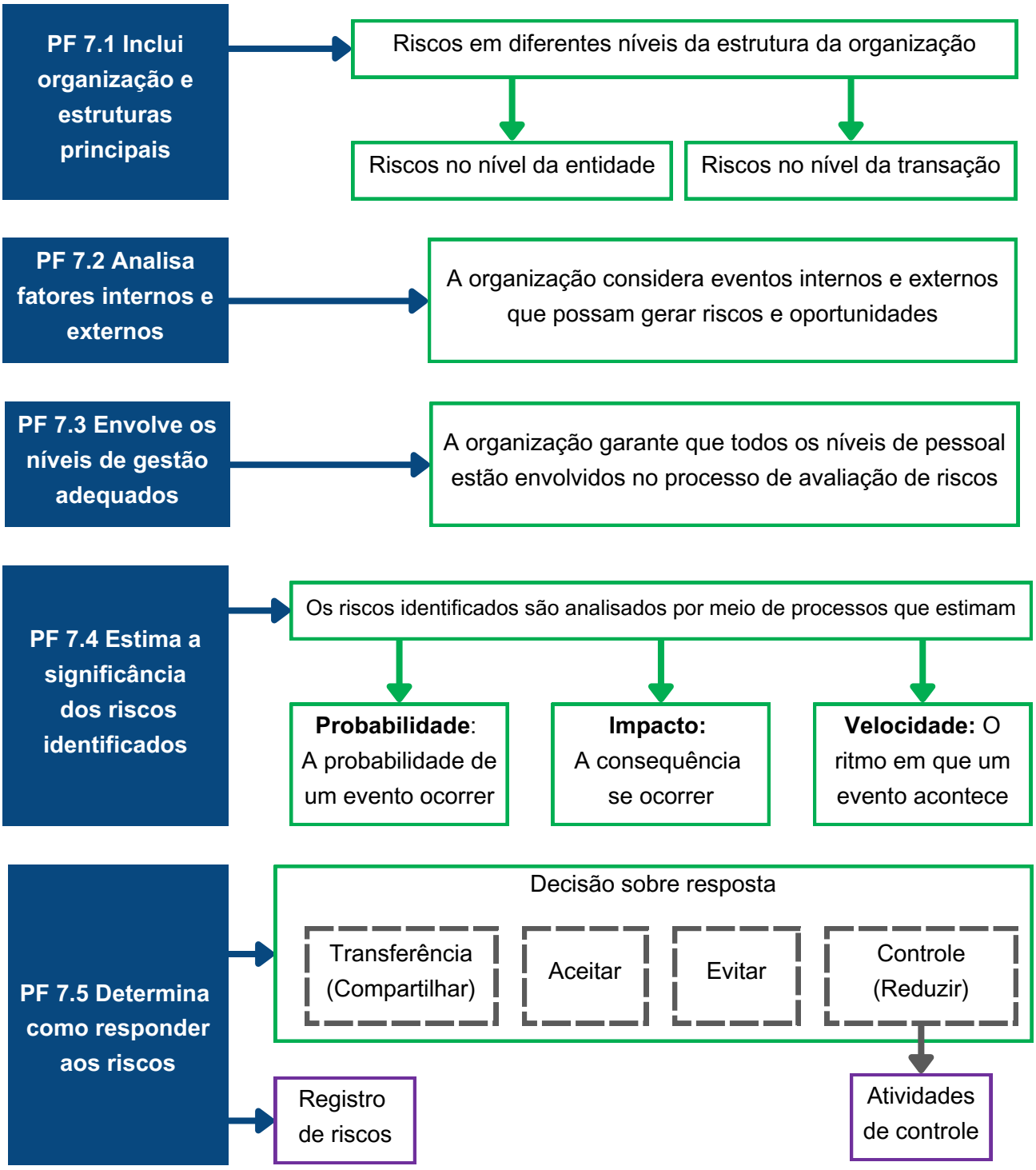
- Os relatórios internos são elaborados pelas unidades dentro da organização quando consideram apropriado fazê-lo.
- Os relatórios internos são preparados com um nível adequado de precisão e refletem as transações subjacentes.
- A alta administração decide qual nível de relatório interno é apropriado para diferentes aspectos do orçamento e da gestão financeira.

A organização especifica objetivos relacionados à compliance com leis e regulamentos externos? Por exemplo:

- Existe uma política explicando como os gestores devem estabelecer objetivos para cumprir os padrões de todo o governo.
- Os objetivos de compliance podem ser amplos e incluir questões ambientais, a necessidade de concorrência, regulamentos de segurança e proteção e políticas fundamentais de pessoal, como salários-mínimos e assédio.
- Os objetivos de compliance estão incluídos na estratégia de alto nível da organização.
- A organização atende a todos os principais objetivos de compliance.
- Existe um alto nível de conscientização na organização sobre a importância dos objetivos de compliance.

Princípio 7. A organização identifica riscos para a consecução de seus objetivos em toda a organização e analisa como base para determinar como esses riscos devem ser gerenciados

Figura 10. Interpretação do Princípio 7



Comentário

Uma vez definidos os objetivos conforme previstos no Princípio 6, a administração deve identificar os riscos para a consecução desses objetivos e analisá-los para determinar como os riscos devem ser gerenciados. O COSO promove o uso da avaliação de risco orientada a eventos, em que os eventos são coisas que podem acontecer e que têm um impacto positivo ou negativo em uma organização: impactos positivos são oportunidades para alcançar objetivos e impactos negativos são riscos para atingir objetivos.

Os riscos devem ser abordados em todos os níveis da organização, desde a avaliação do impacto nas transações (riscos de transação) até a avaliação do impacto na organização como um todo (riscos corporativos). O processo deve avaliar tantos eventos externos (eventos climáticos, distúrbios sociais, roubo de ativos, problemas de fornecimento de energia elétrica) quanto eventos internos (perdas de pessoal, quebra de maquinário, erros cometidos pelo pessoal, etc.). Os gestores devem ser capazes de distinguir eventos/riscos que estão sob seu controle daqueles que estão fora de seu controle.

É importante que o pessoal de todos os níveis esteja envolvido no processo de identificação e avaliação de riscos. Os colaboradores responsáveis pelo processamento de transações podem ter informações vitais sobre riscos que não são conhecidas por seus supervisores.

Tendo identificado eventos que podem representar riscos, a organização deve avaliar a importância de cada risco para garantir que está abordando os riscos mais importantes que enfrenta. A prática comum é avaliar o risco de três maneiras:

- **Probabilidade**, a probabilidade de ocorrência de um evento – por exemplo, as chances de ser atingido por um meteoro ou atropelado por um carro.

- **Impacto**, a consequência ou gravidade se ocorrer – por exemplo, compare as consequências de um pouso forçado de avião com um acidente de carro.

- **Velocidade**, o ritmo em que um evento acontece. Por exemplo, compare o período de alerta para um raio e um grande furacão.

Tendo determinado a importância do risco, a administração deve decidir como responder a ele. Existem quatro respostas principais ao risco:

- **Evitação**. Pare de fazer as coisas que causam risco (onde isso for possível). Isso pode não ser uma opção em algumas organizações do setor público que são obrigadas por lei a realizar atividades inerentemente arriscadas, por exemplo, polícia, bombeiros e serviços de ambulância de emergência.

- **Controle (ou redução)**. Decidir tomar medidas para reduzir a probabilidade ou o impacto do risco. Por exemplo, são implementados controles adicionais para fazer face a um risco grave de fraude por parte dos beneficiários dos serviços sociais.

- **Aceitação**. Decida aceitar as consequências do risco e não tome nenhuma ação para alterar sua probabilidade ou impacto. Isso geralmente será a resposta a quaisquer riscos que (a) tenham impacto mínimo e baixa probabilidade ou (b) ocorram tão lentamente que seja possível responder ao risco em tempo real.

- **Transferência (ou compartilhamento)**. A probabilidade ou o impacto de um risco é compartilhado ou transferido para terceiros. Um exemplo comum é quando uma organização faz um seguro para reembolsar algumas ou todas as suas despesas caso o evento ocorra.

A diferença entre risco inerente e risco residual deve ser claramente compreendida. O **risco inerente** é o risco para uma organização na ausência de quaisquer ações de gerenciamento (resposta ao risco) para alterar a probabilidade ou o impacto do risco. **Risco residual** é o risco que permanece após a resposta da administração ao risco. A avaliação de risco é aplicada primeiro aos riscos inerentes. Uma vez que as respostas aos riscos tenham sido desenvolvidas, a administração considera o risco residual. Observe que quando a resposta é evitar ou aceitar o risco, o risco inerente é o mesmo que o risco residual.

Critérios para avaliar a eficácia dos controles internos

A organização considera riscos em diferentes níveis da organização estrutura? Por exemplo:

- Existe um requisito para processos formais de avaliação de riscos em toda a organização.

- A maioria das unidades organizacionais realiza algum tipo de avaliação de risco.

- Existem registros de risco separados para escritórios regionais e centrais.

- Existem registos de risco separados para unidades organizacionais que funcionam como entidades independentes sem fins lucrativos que cobram pelos seus serviços ou produtos.

- Existem registros de riscos separados para cada unidade operacional e um registro de riscos corporativos para os principais riscos enfrentados pela organização como um todo.

A organização considera eventos internos e externos que possam gerar riscos e oportunidades? Por exemplo:

- Existe uma política formal de avaliação de riscos que explica como identificar e avaliar o impacto de eventos internos e externos.
- Os colaboradores recebem exemplos dos tipos de eventos internos e externos que podem levar a riscos e oportunidades.
- Os colaboradores são treinados em como realizar uma avaliação de risco formal.

A organização garante que todos os níveis de pessoal estão envolvidos no processo de avaliação de riscos? Por exemplo:

- Colaboradores em diferentes níveis realizam reuniões separadas de avaliação de risco.
- As avaliações de risco são sempre realizadas em reuniões envolvendo colaboradores de todos os níveis.

A administração estima a importância dos riscos identificados? Por exemplo:

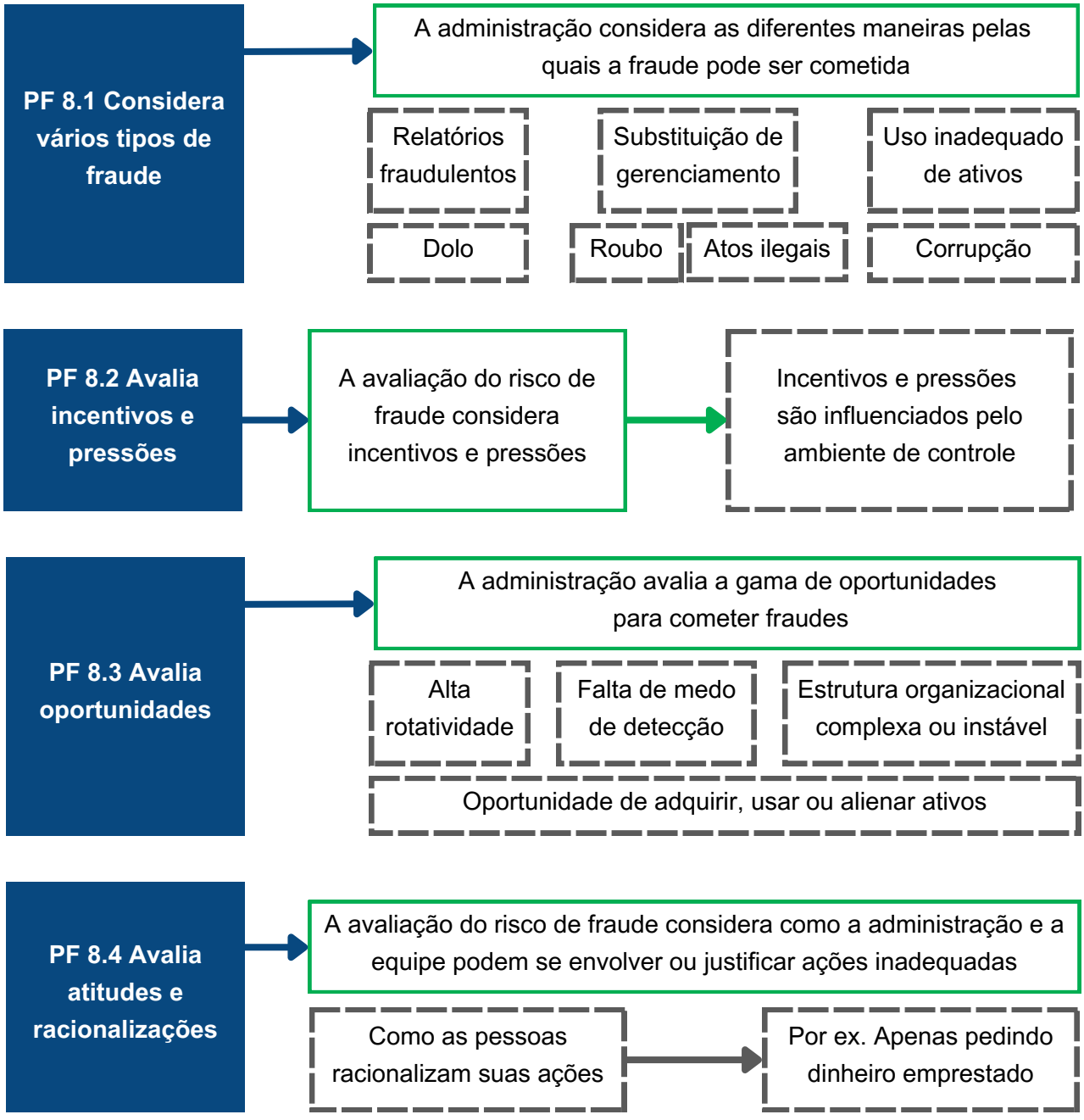
- O registro de riscos contém avaliações da probabilidade, impacto e velocidade de todos os riscos identificados.
- Existe um sistema comum para pontuar riscos em toda a organização para determinar os riscos mais altos enfrentados pela organização, medindo probabilidade, impacto e velocidade.

A administração determinou como responder aos riscos identificados? Por exemplo:

- A política de avaliação de risco fornece quatro possíveis respostas ao risco - evitar, transferir (compartilhar), aceitar ou reduzir (controlar) o risco.
- O registro de risco inclui a resposta de risco acordada e referências a atividades de controle conforme apropriado.
- A administração garante que as respostas aos riscos sejam econômicas, fazendo uso apropriado de todas as quatro respostas aos riscos.

Princípio 8. A organização considera o potencial de fraude na avaliação dos riscos para o alcance dos objetivos

Figura 11. Interpretação do Princípio 8



Comentário

A estrutura COSO atualizada em 2013 inclui um princípio específico sobre a necessidade de abordar o potencial de fraude para enfatizar a necessidade de que isso seja coberto durante o processo de avaliação de risco.

Por que as pessoas cometem fraude e corrupção? A maioria dos policiais dirá que o crime tem dois elementos fundamentais: motivo e oportunidade. Os criminosos equilibram a oportunidade (o ganho envolvido) com o risco de detecção e punição. Quanto maior o ganho, maiores os riscos que eles estão preparados para assumir.

Há uma diferença significativa entre fraude e corrupção. A fraude é um ataque aos ativos da organização, enquanto a corrupção é uma tentativa de influenciar os processos de tomada de decisão de forma a beneficiar terceiros. Como a maioria das organizações possui registros de seus ativos, a ação fraudulenta geralmente é visível dentro da organização. A corrupção, que envolve um terceiro, pode deixar poucos vestígios internamente e é inerentemente mais difícil de identificar e processar. Uma das principais defesas contra a fraude é reduzir a oportunidade de um indivíduo roubar ativos sem detecção – por exemplo, estabelecendo medidas de controle para detectar transações não autorizadas. Uma das principais defesas contra a corrupção é limitar a influência de qualquer indivíduo em decisões que beneficiem terceiros, por exemplo. segregando funções-chave para refletir o princípio de que “quatro olhos” (ou seja, pelo menos duas pessoas) devem revisar todas as transações importantes.

O COSO incentiva os gestores a **considerar os vários tipos de fraude e corrupção existentes.** Esta é uma área em que a auditoria interna possui experiência considerável e, portanto, pode auxiliar a administração na identificação de riscos.

O COSO também destaca **a importância de entender os incentivos, pressões e oportunidades** que podem levar à fraude. Não existe um perfil de pessoas que cometem fraudes e corrupção. Em muitos casos, a fraude é realizada por pessoas que, de outra forma, são bons colegas. É o motivo e a oportunidade que levam ao crime. Fatores de risco comuns incluem:

- mudanças repentinas no estilo de vida;
- indivíduos com graves dificuldades financeiras;
- indivíduos que têm fortes relações pessoais com os principais fornecedores ou contratados;

- colaboradores que raramente tiram licença ou permitem que outros façam seu trabalho; e
- colaboradores que não desejam ser supervisionados ou não cooperam com os supervisores.

Finalmente, é importante avaliar as atitudes dos colaboradores em relação à fraude e corrupção e a forma como eles podem racionalizar suas ações. Por exemplo: “Como esperam que eu sobreviva com os baixos salários que me pagam?”; “Todos são corruptos nesta organização!”; e assim por diante.

Critérios para avaliar a eficácia do controle interno

A administração considera as diferentes maneiras pelas quais a fraude pode ser cometida? Por exemplo:

- Existe uma política antifraude e anticorrupção que explica aos colaboradores o diferentes maneiras pelas quais a fraude e a corrupção podem ocorrer, por exemplo, roubo, engano, uso inapropriado de ativos, relatórios fraudulentos, anulação de controles pela administração e atos ilegais.

- Todos os colaboradores recebem treinamento básico sobre conscientização sobre fraude e corrupção.

- Os casos reais de fraude e corrupção identificados são relatados a todos os colaboradores para aumentar a conscientização sobre as formas pelas quais a fraude pode ser cometida.

A avaliação do risco de fraude considera incentivos e pressões para cometer fraude e corrupção? Por exemplo:

- Todos os colaboradores em cargos gerenciais são obrigados a fornecer uma declaração de sua situação financeira a cada ano.

- Existe adequada segregação de funções para garantir que os gestores não possam tomar decisões sozinhos: o princípio dos quatro olhos é seguido.

- Existem verificações periódicas de conflito de interesses na tomada de decisões.

A administração avaliou a gama de oportunidades para cometer fraude? Por exemplo:

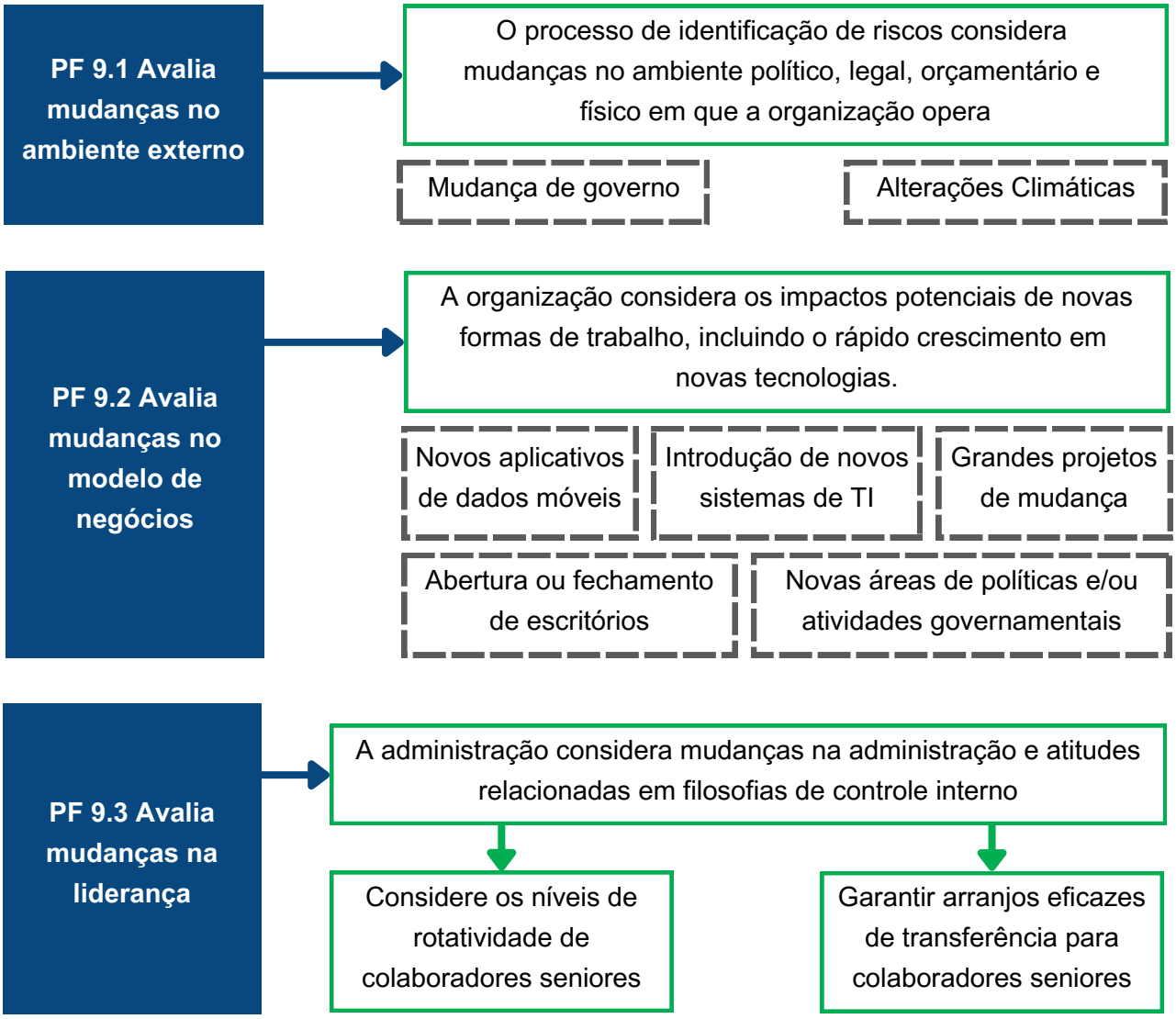
- A gestão inclui avaliações de oportunidades de fraude durante os processos de avaliação de risco.
- Foram identificados os fatores que levam à alta rotatividade de colaboradores em funções-chave.
- A administração identifica posições financeiras de alto risco para níveis adicionais de revisão.
- A administração divulga todos os casos de fraude e corrupção para aumentar o medo de detecção de fraude ou atos corruptos.

A avaliação do risco de fraude considera como a administração e a equipe podem se envolver ou justificar ações inadequadas? Por exemplo:

- Todos os colaboradores tiveram um nível mínimo de treinamento em conscientização sobre fraude e corrupção.
- Há verificações periódicas de comportamento pessoal.
- Existe um comitê interno de práticas antifraude.
- A auditoria interna realiza revisões de terceira linha dos riscos de fraude e corrupção.
- Um registro de riscos inclui áreas de grande risco de fraude e corrupção.

Princípio 9. A organização identifica e avalia as mudanças que podem impactar significativamente o sistema de controle interno

Figura 12. Interpretação do Princípio 9



Comentário

O COSO destaca a importância de avaliar os riscos que surgem devido a mudanças na forma como uma organização opera. Os riscos decorrentes da mudança são tão amplos e difundidos que o COSO recomenda que sejam considerados como um princípio separado de controle interno. O COSO recomenda que os gestores se concentrem em três tipos de mudança.

Mudança que acontece fora da organização - o ambiente externo. Nenhuma organização, pública ou privada, existe no vácuo. O que acontece fora das organizações do setor público pode ter um impacto significativo na maneira como elas operam ou mesmo em sua própria existência. Por exemplo, mudanças na lei podem resultar na adição ou remoção de atividades importantes; uma grande campanha de mídia social pode ajudar ou atrapalhar a implementação de políticas-chave; etc.

Mudanças na forma de trabalhar das organizações – novos modelos de negócios. Há sempre um aumento do risco associado a novas formas de trabalho. Por exemplo, a introdução de nova tecnologia; abrir ou fechar escritórios; ou aumentar o nível de tomada de decisão descentralizada.

Mudanças na liderança da organização. A pessoa que lidera uma organização tem um grande impacto na cultura dessa organização e, consequentemente, no importante ambiente de controle. Portanto, o COSO recomenda que as mudanças na liderança sejam consideradas durante o processo de avaliação de riscos.

Critérios para avaliar a eficácia do controle interno

O processo de identificação de riscos considera mudanças no ambiente político, legal, orçamentário e físico em que a organização opera? Por exemplo:

- A administração considera mudanças na (a) liderança política (governo); (b) as direções econômicas/políticas/geográficas globais; (c) o quadro regulamentar; (d) grande reestruturação do setor público – fusão de ministérios/agências; e (e) mudanças contínuas ou esperadas nas práticas da administração pública (ou seja, GFP/controle interno do setor público – PIC).

- A gestão considera as mudanças resultantes da disponibilidade de recursos (redução do número de servidores públicos ou outros recursos orçamentários).

- A administração considera mudanças no ambiente externo além do controle da organização, como impactos climáticos severos.

- Existe uma unidade dentro da organização que é responsável por monitorar a mudança.

O processo de identificação de riscos considera os impactos potenciais de novas formas de trabalho, incluindo o rápido crescimento em novas tecnologias? Por exemplo:

- A administração considera os principais projetos de mudança que resultam em mudanças nas principais estruturas, funções, papéis, serviços e produtos entregues.
- A administração considera mudanças para novas tecnologias - tecnologias disruptivas, incluindo dados móveis e seu impacto nos processos internos e controle interno.
- Existem processos claros para lidar com tecnologias de informação e comunicação/riscos de segurança cibernética e disponibilidade operacional por meio de planejamento de continuidade de negócios e/ou planejamento de recuperação de desastres.
- A administração considera a capacidade de pessoal relevante para novas funções e objetivos.
- Existe uma unidade dentro da organização que é responsável por monitorar a mudança.

O processo de identificação de riscos considera mudanças na gestão e atitudes relacionadas nas filosofias de controle interno? Por exemplo:

- A administração considera o impacto de novos gestores com uma nova visão de PIC e diferentes atitudes em relação aos controles.
- A administração considera o impacto de altos níveis de rotatividade em cargos de gestão em geral.
- Existem trabalhos específicos que possuem acordos formais de transferência para garantir que as informações sobre as principais atividades de controle sejam passadas de um gestor para outro.
- Existe uma unidade dentro da organização que é responsável por monitorar a mudança.

ANEXO B3. ATIVIDADES DE CONTROLE

Este anexo enfoca o Componente 3 – Atividades de Controle, que são os controles implementados para responder aos riscos, e as políticas e procedimentos que ajudam a garantir que as diretrizes de gerenciamento sejam cumpridas. Há muitas opções abertas à administração para garantir que os objetivos sejam alcançados e que os riscos sejam tratados, se necessário, por meio de atividades de controle. O objetivo é minimizar o custo dos controles de acordo com os riscos envolvidos. Os controles não devem ser apenas eficazes, mas também econômicos. Além disso, a existência de muitos controles pode realmente ter um impacto negativo. Por exemplo, um relatório que é revisado por várias pessoas em uma cadeia pode não ser totalmente revisado em detalhes por qualquer indivíduo porque cada um acredita que outros estão realizando a principal ação de controle.

O COSO identifica **três princípios dentro deste componente**, que estão listados na tabela abaixo.

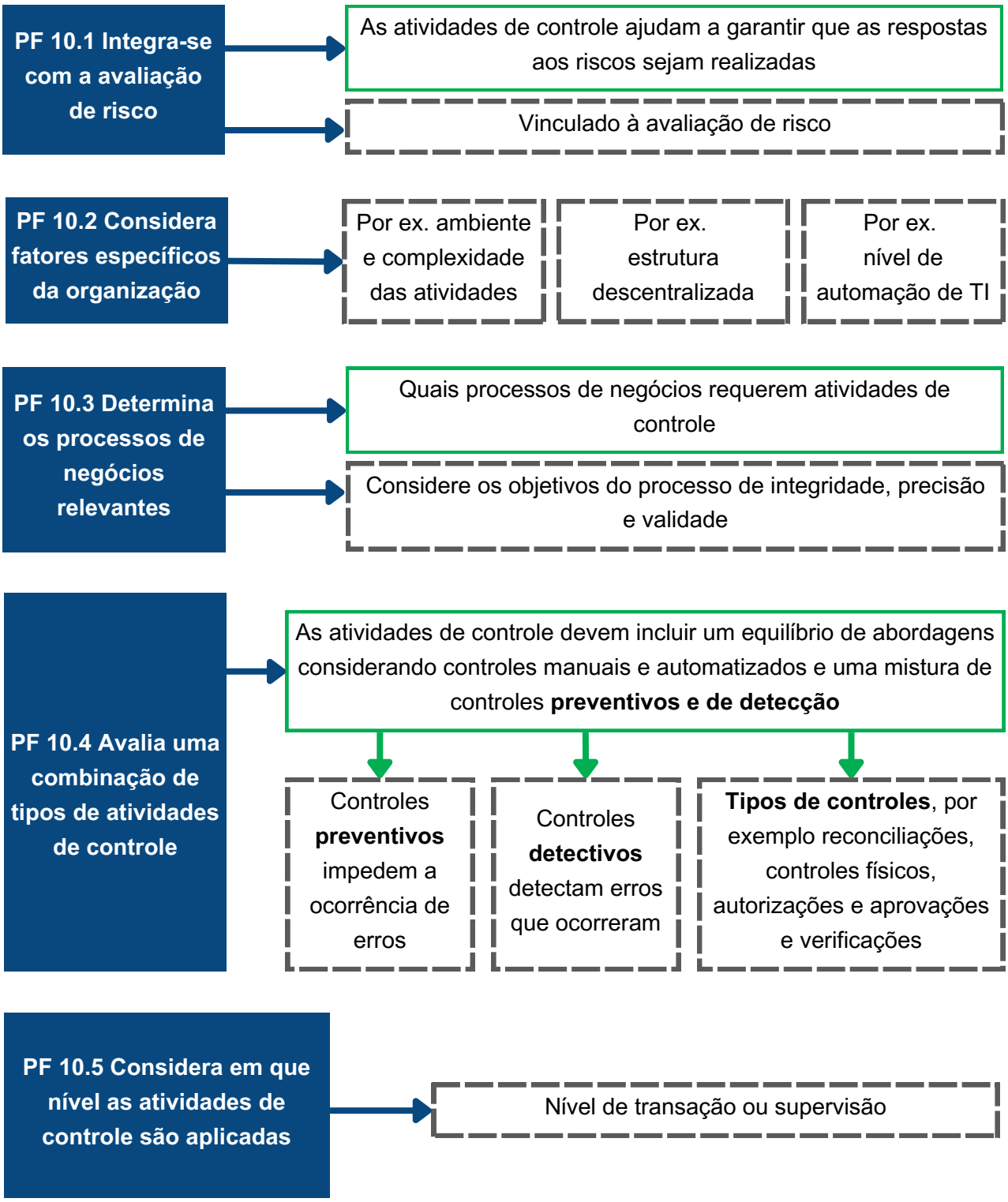
Tabela 5. Os Princípios e Pontos de Foco do Componente 3 – Atividades de Controle

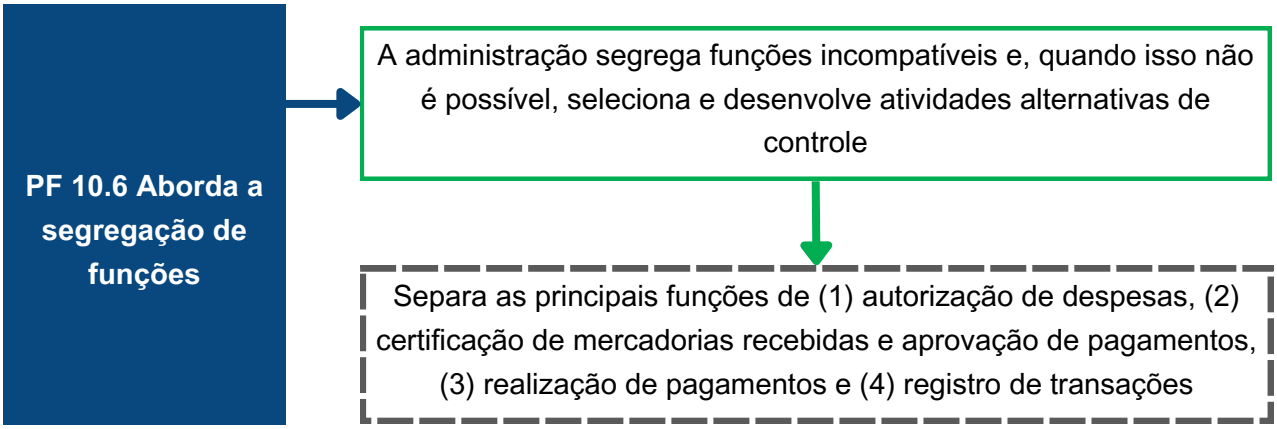
Princípio	Pontos de Foco
10 A organização desenvolve atividades de controle que contribuem para a mitigação dos riscos para o alcance dos objetivos em níveis aceitáveis.	10.1. Integra-se com a avaliação de risco.
	10.2. Considera fatores específicos da organização.
	10.3. Determina os processos de negócios relevantes.
	10.4. Avalia uma combinação de tipos de atividades de controle.
	10.5. Considera em que nível as atividades são aplicadas.
	10.6. Aborda a segregação de funções.

Princípio	Pontos de Foco
11 A organização seleciona e desenvolve atividades gerais de controle sobre a tecnologia para apoiar o alcance dos objetivos.	11.1. Determina a dependência entre o uso de tecnologia em processos de negócios e controles gerais de tecnologia.
	11.2. Estabelece atividades relevantes de controle de infraestrutura de tecnologia.
	11.3. Estabelece atividades relevantes de controle do processo de gerenciamento de segurança.
	11.4. Estabelece atividades relevantes de controle de processo de aquisição, desenvolvimento e manutenção de tecnologia.
12 A organização desenvolve atividades de controle por meio de políticas que estabelecem o que é esperado e em procedimentos que colocam as políticas em ação.	12.1. Estabelece políticas e procedimentos para apoiar a implantação das diretrizes da administração.
	12.2. Estabelece responsabilidade e responsabilidade pela execução de políticas e procedimentos.
	12.3. Executa em tempo hábil.
	12.4. Toma ação corretiva.
	12.5. Realiza usando pessoal competente.
	12.6. Reavalia políticas e procedimentos.

Princípio 10. A organização desenvolve atividades de controle que contribuem para a mitigação dos riscos para o alcance dos objetivos a níveis aceitáveis

Figura 13. Interpretação do Princípio 10





Comentário

As atividades de controle são políticas e procedimentos (as ações das pessoas para implementar as políticas diretamente ou usando TI) para garantir que as respostas aos riscos sejam realizadas e os riscos para alcançar os objetivos da organização sejam tratados. **Esse vínculo com a avaliação de riscos é fundamental para garantir que os controles abordem os riscos mais importantes.**

A administração precisa determinar quais processos de negócios requerem atividades de controle e desenvolver uma combinação de controles preventivos e de detecção:

- Os **controles preventivos** são projetados para impedir que erros e omissões ocorram antes que as transações aconteçam (por exemplo, uma verificação de validação de que os pagamentos estão sendo feitos apenas para empresas que possuem um registro de fornecedor no sistema de TI).

- Os **controles de detecção** são projetados para identificar erros que já ocorreram (por exemplo, uma verificação que identifica fornecedores que foram pagos duas vezes).

Todos os controles preventivos e alguns controles de detecção operam na primeira linha de defesa, enquanto a maioria dos controles de detecção opera como uma segunda linha de defesa.

A administração frequentemente usará muitos tipos diferentes de controles, por exemplo:

- **Controles de processamento de informações**: incluem verificações de dados inseridos, sequências numéricas de transações e controles de acesso a dados, arquivos e software.

- **Controles físicos**: equipamentos, estoques, dinheiro e valores mobiliários são fisicamente protegidos, contados periodicamente e comparados aos registros de controle.

- **Relatórios/rotinas de exceção**: muitos sistemas de controle (principalmente sistemas computadorizados) rejeitarão transações que falham em determinados testes que exigem alguma forma de intervenção/aprovação da administração antes que a transação possa ser processada.

- **Ações de gerenciamento direto**: revisões regulares de gerenciamento de linha de, por exemplo, relatórios de desempenho, relatórios de exceções e reconciliações entre diferentes conjuntos de dados.

- **Revisões de alto nível**: Revisões da alta administração do desempenho real em relação a orçamentos, previsões e períodos anteriores. Isso inclui o acompanhamento das principais iniciativas para medir até que ponto as metas estão sendo alcançadas.

- **Medidas e indicadores de desempenho**: Diferentes conjuntos de dados (por exemplo, dados financeiros e operacionais) são comparados e as relações entre eles analisadas. Ao identificar resultados inesperados ou tendências incomuns, a administração pode identificar pontos fracos nos controles. Investigação e ação corretiva servem como atividade de controle.

A segregação de funções é um elemento-chave das atividades de controle. Papéis e responsabilidades são divididos ou (“segregados”) entre diferentes pessoas para reduzir o risco de erros ou ações inadequadas, como fraude e roubo. Por exemplo, diferentes indivíduos devem ser responsáveis por (1) autorizar despesas; (2) certificar bens e serviços recebidos e aprovar o pagamento; (3) fazer pagamentos; e (4) transações de registro.

Os controles operam em diferentes níveis. Os controles de nível inferior geralmente operam no nível da transação e podem ser considerados como a primeira linha de defesa contra riscos. No entanto, controles de nível superior, como indicadores de desempenho e relatórios de exceção, fornecem aos gestores um nível muito maior de garantia de que os sistemas estão funcionando com eficiência e também podem ser usados pela segunda linha de defesa. Os gestores seniores geralmente se concentram em controles de nível superior sempre que possível.

Critérios para avaliar a eficácia do controle interno

A organização garante que as atividades de controle sejam integradas à avaliação de riscos? Por exemplo:

- Todos os registros de riscos incluem referências às atividades de controle que visam reduzir os riscos inerentes a um nível aceitável.

- Existe um registro de riscos corporativos que identifica os principais riscos enfrentados pela organização e as principais atividades de controle implementadas para lidar com esses riscos.

A organização considerou fatores específicos da organização (como o nível de descentralização e a extensão da automação de TI) no desenvolvimento de atividades de controle? Por exemplo:

- A organização entende e aplica o conceito do modelo de três linhas ao projetar suas atividades de controle.

- A organização usa o modelo de três linhas para estabelecer controles efetivos sobre atividades descentralizadas: há um conjunto comum de orientações para gestores de escritórios regionais sobre os papéis da segunda e terceira linhas em relação às atividades regionais.

A organização determinou quais processos de negócios requerem atividades de controle? Por exemplo:

- A compreensão de quais processos de negócios requerem atividades de controle varia do básico ao completo, dependendo da maturidade organizacional. O nível básico inclui políticas que especificam quais tipos de contratos exigem licitação competitiva e processos críticos para a preparação de demonstrações financeiras precisas.

- Os objetivos dos processos de negócios cobrem **integridade** (que todas as transações sejam processadas), **precisão** (que as transações sejam avaliadas e registradas corretamente) e **validade** (que as transações representem despesas ou receitas legítimas da organização e tenham sido devidamente autorizadas de acordo com o orçamento).

A organização tem um equilíbrio de abordagens considerando controles manuais e automatizados e uma mistura de controles preventivos e de detecção? Por exemplo:

- Existe uma compreensão clara das diferenças entre controles preventivos e de detecção e uma abordagem equilibrada para o uso de cada tipo de controle.
- A administração faz pleno uso de diferentes tipos de controles, por ex. reconciliações, controles físicos, autorizações e aprovações e verificações de terceiros.
- Tentativas básicas de redução de custos são feitas limitando as verificações de transações abaixo de um determinado valor financeiro.
- A administração avalia o custo-benefício de diferentes atividades de controle antes de determinar quais atividades de controle devem ser implementadas.

A organização considerou em que nível as atividades de controle devem ser aplicadas? Por exemplo:

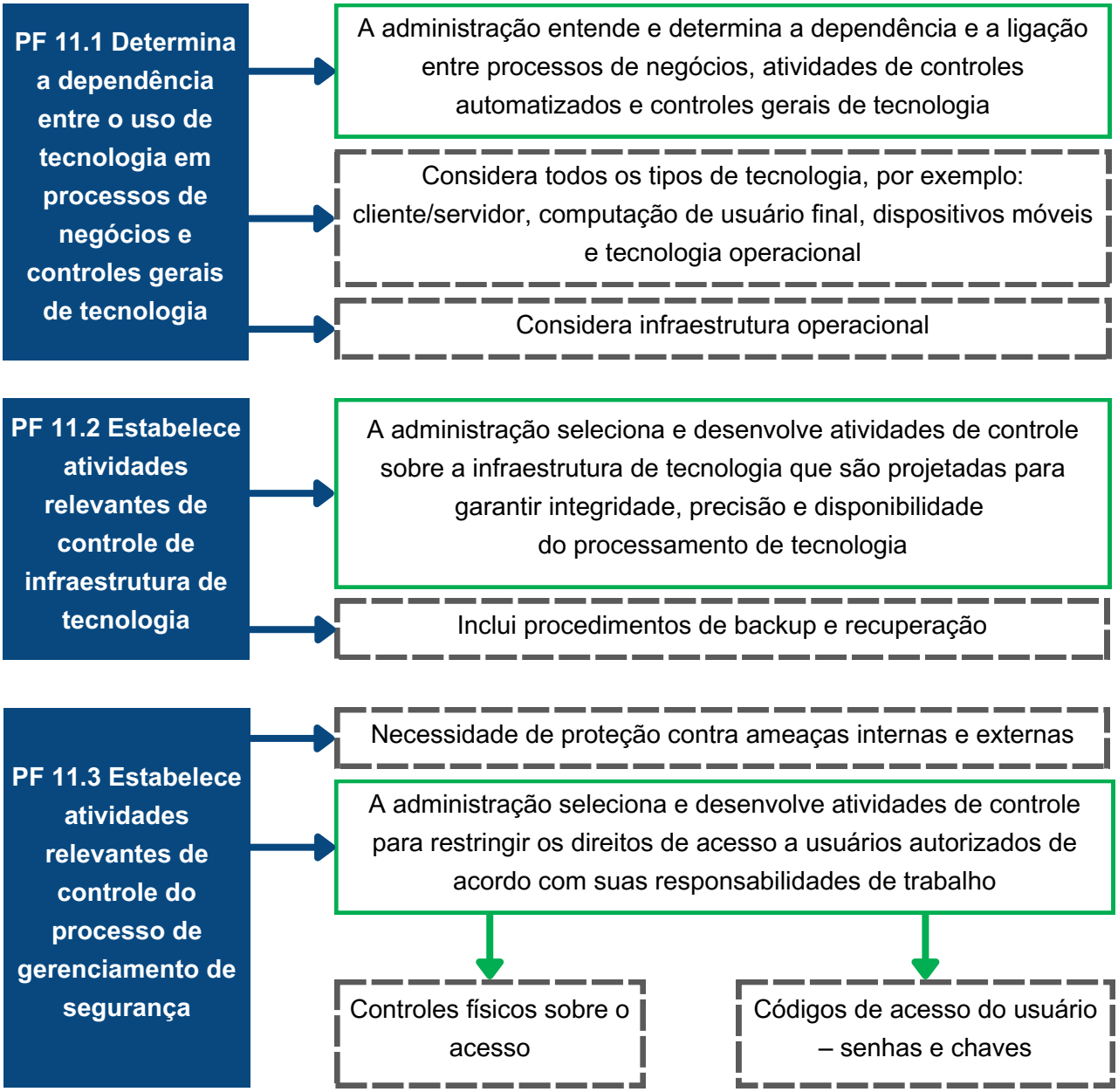
- Existem requisitos separados para atividades de controle nos níveis de transação e supervisão.
- Sempre que possível, a administração concentra os principais controles no nível de supervisão.

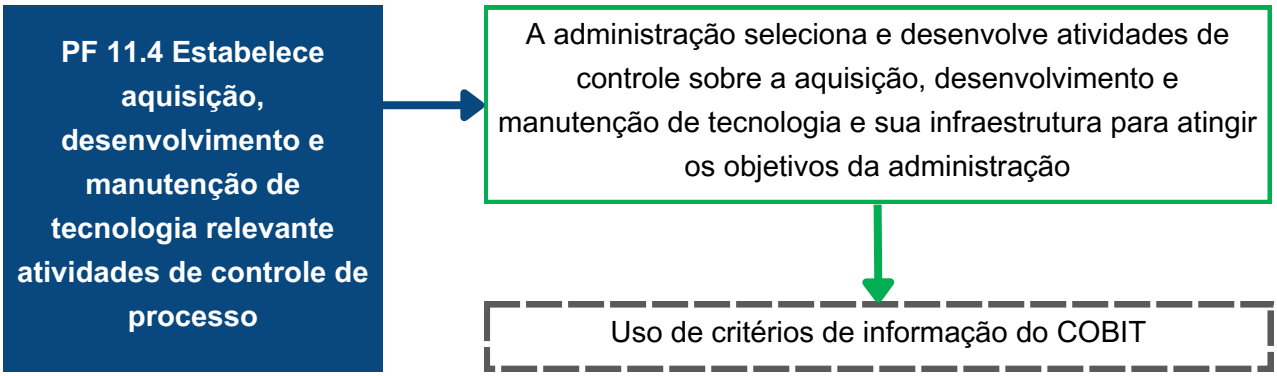
A administração segregou funções incompatíveis e, quando isso não é possível, selecionou e desenvolveu atividades alternativas de controle? Por exemplo:

- A administração identificou quatro funções principais que devem ser segregadas – (1) autorizar gastos, (2) certificar bens recebidos e aprovar pagamentos, (3) efetuar pagamentos e (4) registrar transações.
- Há verificações adicionais por uma unidade de supervisão de segunda linha quando a segregação não é prática devido ao tamanho da unidade de negócios.
- A auditoria interna revisa a adequação da segregação de funções como parte da terceira linha de defesa.

Princípio 11. A organização seleciona e desenvolve atividades gerais de controle sobre a tecnologia para apoiar o alcance dos objetivos

Figura 14. Interpretação do Princípio 11





Comentário

A maioria das organizações é altamente dependente de sistemas de informação. Os controles sobre os sistemas de informação são, portanto, muito importantes. No entanto, os conceitos subjacentes de controle, como identificação de eventos, avaliação de riscos, resposta a riscos e desenvolvimento e implementação de atividades de controle econômicas, são os mesmos para sistemas manuais e baseados em TI.

A administração precisa entender e determinar a dependência e a ligação entre processos de negócios, atividades de controle automatizado e controles gerais de tecnologia. Os principais elementos de TI em uma organização são:

- **Infraestrutura de TI**. Servidores, redes, internet, Wi-Fi, sistema operacional e software aplicativo.
- **Computação pessoal**. Uso comercial de dispositivos móveis e laptops, uso de planilhas e outros arquivos e aplicativos.
- **TI terceirizada**. Uso de computação em nuvem, provedores de serviços externos, backup e armazenamento.
- **Governança de TI**. A estrutura criada para organizar e gerenciar a função de TI.

Existem dois tipos principais de atividades de controle que buscam atender aos objetivos de processamento de informações de integridade, precisão e validade:

- **Atividades de controle de aplicativos** que incluem autorizações, verificações, reconciliações, controles de acesso físico e supervisão de processos.
- **Controles gerais de tecnologia** sobre infraestrutura e operações, segurança de dados e software e ciclo de vida de desenvolvimento do sistema.

Este princípio COSO concentra-se nas **atividades gerais de controle sobre a tecnologia** e especificamente nos controles sobre a infraestrutura de TI (incluindo planos de backup), segurança de TI (acesso a sistemas e aplicativos de TI) e aquisição e desenvolvimento de novas tecnologias. Os controles relacionados a aplicativos específicos geralmente seriam considerados como parte da realização dos objetivos da política para a qual o aplicativo específico foi projetado. Por exemplo, os controles em um aplicativo de TI para processar solicitações de passaportes devem ser projetados para atender aos riscos relacionados ao objetivo de emissão de passaportes.

Critérios para avaliar a eficácia do controle interno

A administração determina a dependência e a ligação entre as atividades de controle de processos de negócios e os controles gerais de tecnologia? Por exemplo:

- Existe uma política de TI separada que identifica todos os principais elementos de TI em uso na organização. A política inclui consideração de tecnologia cliente/servidor, armazenamento de dados baseado em nuvem, computação de usuário final, dispositivos móveis e sistemas operacionais.

- A administração entende e determina a dependência e a ligação entre as atividades de controles automatizados dos processos de negócios e os controles gerais de tecnologia.

- A administração usa a estrutura[6] de Objetivos de Controle para Tecnologia da Informação e Relacionada (COBIT) 5 para a governança e gerenciamento de sistemas e processos de TI em toda a entidade.

A administração estabelece controles de informações de tecnologia relevantes? Por exemplo:

- A administração seleciona e desenvolve atividades de controle sobre a infraestrutura de tecnologia que são projetadas para garantir integridade, precisão e disponibilidade do processamento de tecnologia.

- Existem procedimentos diários de backup e recuperação claramente definidos para todos os dados importantes da organização.

- Existem procedimentos como geradores de energia de backup para garantir um alto nível de disponibilidade dos sistemas de TI corporativos.

[6] Estrutura criada pela Information Systems Audit and Control Association para governança e gerenciamento de TI

A administração estabeleceu atividades relevantes de controle do processo de gerenciamento de segurança? Por exemplo:

- A administração seleciona e desenvolve atividades de controle para restringir os direitos de acesso a usuários autorizados de acordo com suas responsabilidades de trabalho, usando controles físicos sobre o acesso a escritórios com infraestrutura de TI e senhas de usuário para acessar sistemas de TI.

- Controles de segurança de TI mais rígidos incluem alterações regulares nas senhas de acesso e o uso de convenções de nomenclatura de senhas fortes.

- Idealmente, existem limitações estritas e automáticas de acesso do usuário apenas aos aplicativos que são essenciais para o desempenho das funções.

A administração seleciona e desenvolve atividades de controle sobre a aquisição, desenvolvimento e manutenção de tecnologia e sua infraestrutura para atingir os objetivos da administração? Por exemplo:

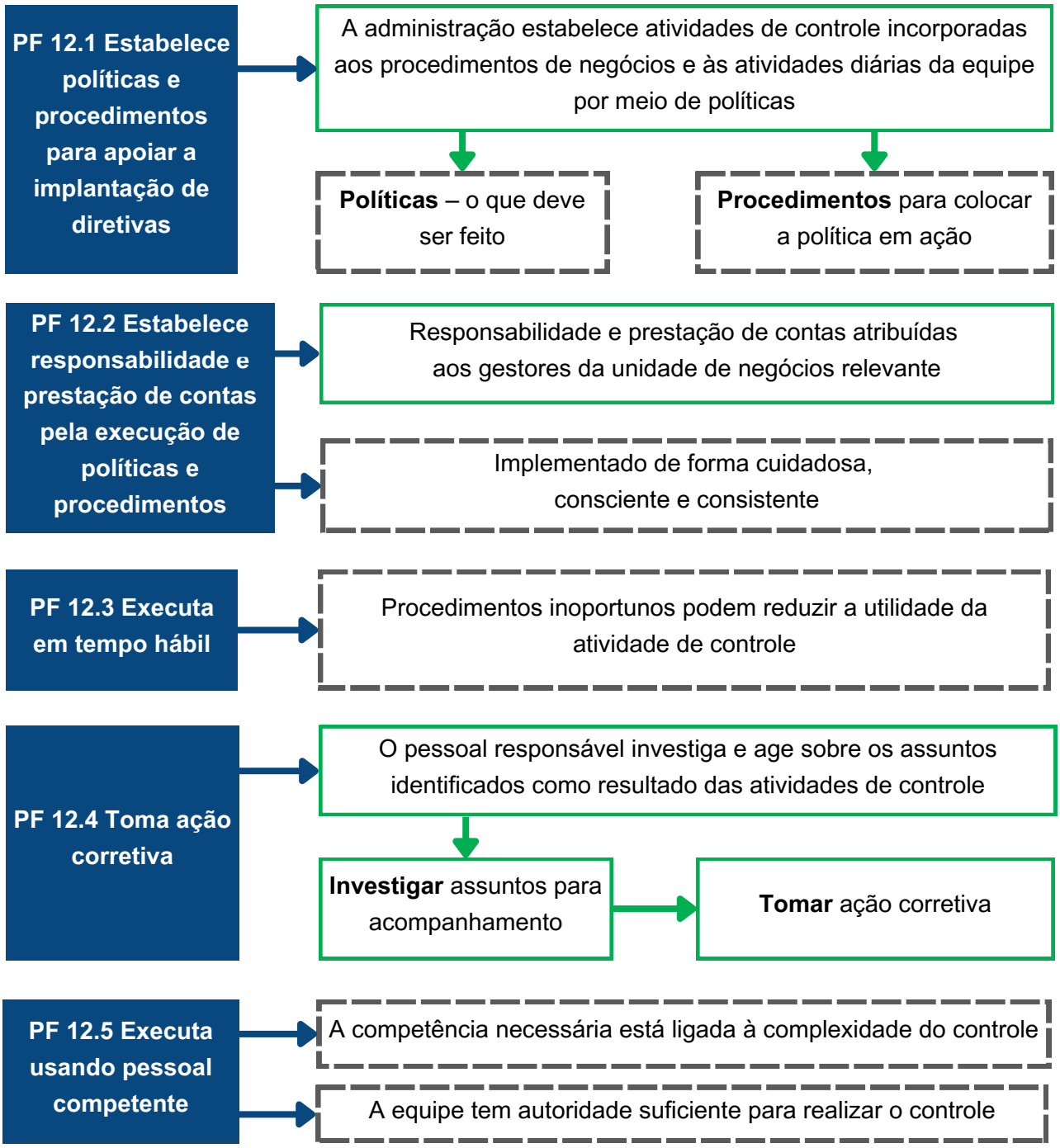
- Uma unidade de TI especializada é responsável pela aquisição, desenvolvimento e manutenção dos processos de TI.

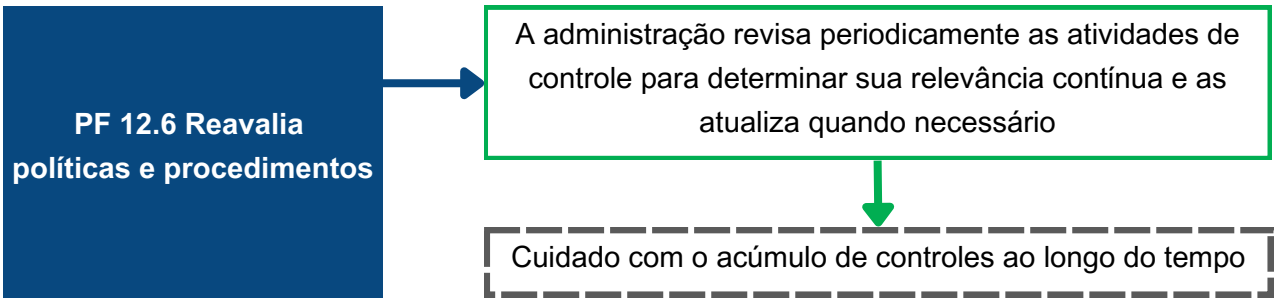
- Um comitê de alto nível supervisiona os desenvolvimentos de TI para a organização como um todo.

- A organização segue a estrutura COBIT 5 para todas as suas aquisições e alienações de TI.

Princípio 12. A organização implementa atividades de controle por meio de políticas que estabelecem o que é esperado e em procedimentos que colocam as políticas em prática

Figura 15. Interpretação do Princípio 12





Comentário

As atividades de controle consistem em **políticas** que descrevem o que deve ser feito e os **procedimentos de controle** que colocam a política em ação. Os procedimentos de controle geralmente têm dois elementos: (i) o próprio processo de controle - o que a pessoa faz; e (ii) a evidência de que o controle foi realizado – geralmente uma assinatura da pessoa que está realizando o controle. A assinatura é apenas um elemento de um procedimento de controle (por exemplo, os supervisores devem assinar todas as autorizações de viagem). São as ações dos supervisores antes de assinarem (o próprio processo de controle) que contam.

A responsabilidade e prestação de contas pela implementação de atividades de controle precisam ser claramente atribuídas. As políticas de controle devem ser implementadas de forma cuidadosa, consciente e consistente. Os procedimentos não são úteis se forem executados mecanicamente ou sem um foco contínuo nítido. Os procedimentos de controle devem ser realizados no momento apropriado. Erros ou problemas identificados como resultado do procedimento devem ser investigados e ações corretivas apropriadas devem ser tomadas.

As atividades de controle também devem ser realizadas por pessoal competente para realizar o procedimento de controle. Por exemplo, seria necessário um eletricista qualificado para realizar verificações mensais do funcionamento de um alarme contra roubo em um depósito. A equipe também pode precisar de um nível definido de autoridade para realizar um controle conjunto. Por exemplo, não seria apropriado que um funcionário aprovasse a solicitação de viagem de seu supervisor.

Os sistemas de controle interno se degradam com o tempo. Muitas organizações experimentam “deslizamento de controle” onde novos controles são adicionados sem considerar a eficácia das atividades de controle existentes. As funções na segunda linha de controle devem ser encarregadas de revisar as atividades de controle periodicamente para determinar sua relevância contínua, fazendo as alterações necessárias.

Critérios para avaliar a eficácia do controle interno

A administração estabeleceu políticas e procedimentos para apoiar a implantação das diretrizes da administração? Por exemplo:

- Existe um conjunto de políticas que identificam o que deve ser feito em termos de controle.
- Existe documentação dos procedimentos (etapas) a serem seguidos para implementação da política.
- Há treinamento obrigatório para a equipe na implementação de controles-chave.

A administração estabeleceu responsabilidade e responsabilidade pela execução de políticas e procedimentos? Por exemplo:

- A responsabilidade por cada elemento do processo de controle é atribuída a indivíduos nomeados.
- Gestores e colaboradores recebem treinamento sobre a importância de implementar controles de forma cuidadosa, consciente e consistente.

A organização realiza atividades de controle em tempo hábil? Por exemplo:

- Existem padrões predefinidos para o tempo necessário para realizar atividades críticas de controle, como o tempo para processar pagamentos ou as datas em que as reconciliações bancárias devem ser concluídas.
- Existem relatórios regulares para supervisores e gestores sobre a pontualidade do processamento de negócios.

A organização toma ações corretivas sobre questões identificadas como resultado das atividades de controle? Por exemplo:

- Existem procedimentos para ações corretivas, mas o nível de adesão depende da maturidade da organização.
- Os supervisores de nível superior devem autorizar pessoalmente o processamento de todas as transações rejeitadas pelas verificações de validação de TI.
- Existem relatórios regulares para supervisores e gestores sobre áreas onde não foram tomadas ações corretivas.

A organização realiza atividades de controle com pessoal competente? Por exemplo:

- O nível de competência e autoridade necessários para realizar cada atividade de controle é claramente definido.
- Os gestores e colaboradores estão cientes da competência e autoridade necessárias para realizar os controles de forma eficaz.
- Despesas acima de limites financeiros predeterminados devem ser autorizadas por colaboradores mais graduados.

A organização revisa periodicamente as atividades de controle para determinar sua relevância contínua, atualizando-as quando necessário? Por exemplo:

- A administração analisa regularmente a relevância contínua das atividades de controle.
- Existe um cronograma claro para revisões da relevância contínua das atividades de controle.
- A alta administração concorda com a auditoria interna sobre a frequência das auditorias baseadas em sistemas dos principais processos de negócios.
- Todas as delegações financeiras têm uma cláusula de caducidade que especifica a data em que devem ser revisadas para determinar sua relevância contínua.

ANEXO B4. INFORMAÇÃO E COMUNICAÇÃO

Este anexo se concentra no Componente 4 – Informação e Comunicação, que garante que as informações pertinentes sobre as atividades de uma entidade sejam identificadas, capturadas e comunicadas de forma e prazo que permitam às pessoas cumprir suas responsabilidades:

- A comunicação é o processo iterativo contínuo de fornecer, compartilhar e obter as informações necessárias.
- Informação são os dados que são combinados e resumidos com base na relevância para os requisitos de informação.

O COSO identifica **três princípios dentro deste componente**, que estão listados na tabela abaixo.

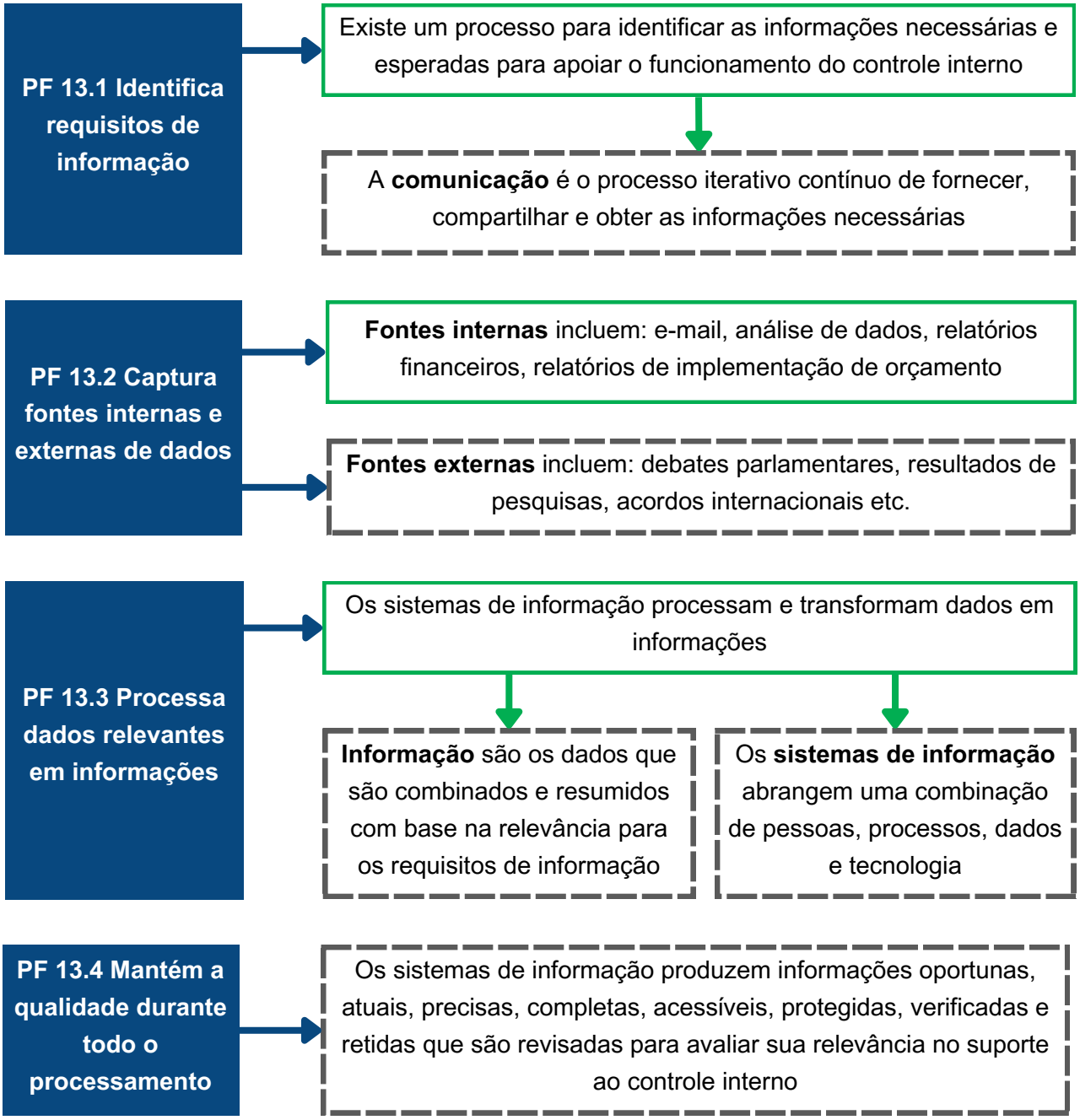
Tabela 6. Os Princípios e Pontos de Foco do Componente 4 – Informação e Comunicação

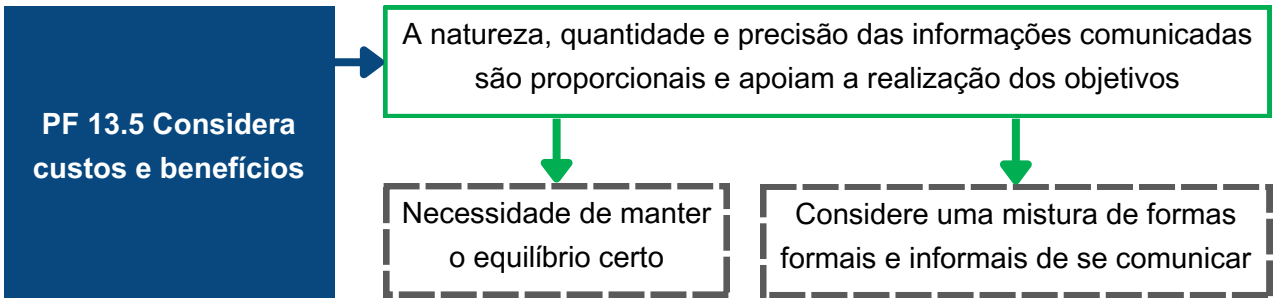
Princípio	Pontos de Foco
13 A organização obtém ou gera e usa informações relevantes e de qualidade para apoiar o funcionamento do controle interno.	13.1. Identifica os requisitos de informação.
	13.2. Captura fontes internas e externas de dados.
	13.3. Processa dados relevantes em informações.
	13.4. Mantém a qualidade durante todo o processamento.
	13.5. Considera custos e benefícios.

Princípio	Pontos de Foco
14 A organização comunica internamente informações, incluindo objetivos e responsabilidades de controle interno, necessárias para apoiar o funcionamento do controle interno.	14.1. Comunica informações de controle interno.
	14.2. Comunica-se com entidades reguladoras.
	14.3. Fornece linhas de comunicação separadas.
	14.4. Seleciona métodos relevantes de comunicação.
15 A organização se comunica com partes externas sobre assuntos que afetam o funcionamento do controle interno.	15.1. Comunica-se com partes externas.
	15.2. Ativa a comunicação de entrada.
	15.3. Comunica-se com entidades reguladoras.
	15.4. Fornece linhas de comunicação separadas.
	15.5. Seleciona métodos relevantes de comunicação.

Princípio 13. A organização obtém ou gera e usa informações relevantes e de qualidade para apoiar o funcionamento do controle interno

Figura 16. Interpretação do Princípio 13





Comentário

A organização precisa identificar seus requisitos de informação e garantir que as informações relevantes sejam obtidas de fontes internas e externas.

A organização deve capturar e usar dados históricos e atuais conforme necessário para dar suporte a controles internos eficazes, particularmente em seu monitoramento na segunda linha de defesa. Especificamente:

- A infraestrutura de informação converte dados brutos em informações relevantes que auxiliam o pessoal no desempenho de suas responsabilidades.
- As informações são fornecidas de forma prontamente utilizável e em tempo hábil de acordo com necessidades específicas – incluindo a necessidade de identificar, avaliar e responder a riscos.
- Os dados são confiáveis e fornecidos no momento certo e no local certo para permitir uma tomada de decisão eficaz.

Critérios para avaliar a eficácia do controle interno

A administração estabeleceu um processo para identificar as informações necessárias e esperadas para apoiar o funcionamento do controle interno? Por exemplo:

- As necessidades de informação dos principais controles são especificadas em manuais e procedimentos internos.
- O processo de comunicação de fornecimento e compartilhamento de informações funciona bem.
- Pessoal individual recebe a responsabilidade de (a) definir as necessidades de informação e (b) gerar os dados para atender a essas necessidades.

A **organização possui sistemas de informação que processam e transformam dados internos e externos em informação?** Por exemplo:

- Fontes internas de dados incluem e-mails, análise de dados, relatórios financeiros e relatórios de implementação orçamentária.
- Fontes externas de dados incluem debates públicos ou parlamentares, pronunciamentos do governo, cobertura da imprensa, resultados de pesquisas externas e acordos internacionais.
- A organização possui sistemas de coleta e comunicação de dados internos e externos.
- Existe um sistema único para processar todos os dados contábeis da organização.
- Ao longo do tempo, o processo de captura e comunicação de informações é automatizado.

A organização processa dados relevantes em informações? Por exemplo:

- A organização possui sistemas de informação para processar dados críticos em informações utilizáveis para os gestores.
- Os dados que não atendem aos critérios de precisão não são incluídos nos relatórios gerenciais.

A organização mantém a qualidade em todo o seu processamento? Por exemplo:

- Os sistemas das organizações são projetados para produzir informações oportunas, atuais, precisas, completas, acessíveis, protegidas, verificadas e retidas.
- Todos os sistemas de entrada de dados financeiros têm maneiras de validar os dados originais (por exemplo, por meio de digitação dupla, aprovação do supervisor etc.) antes que os dados sejam aceitos para processamento.

A **organização considera os custos e benefícios da coleta e disseminação de informações?** Por exemplo:

- A administração revisa a natureza, quantidade e precisão das informações comunicadas para verificar se os custos da coleta de informações são consistentes com os benefícios obtidos.

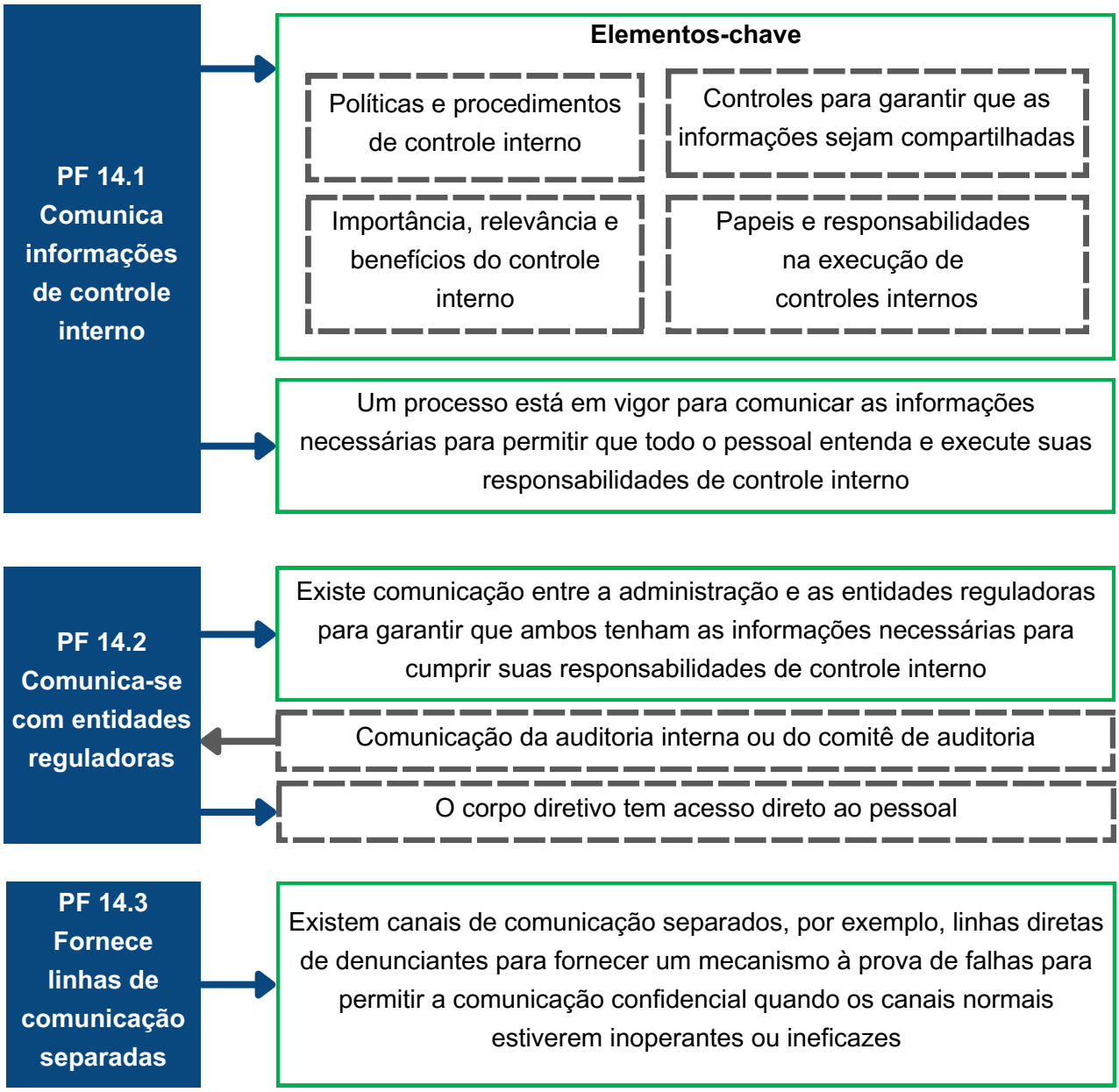
- A organização identifica o custo de produzir relatórios importantes sobre eficácia do controle, incluindo os custos diretos dos exames de auditoria interna.

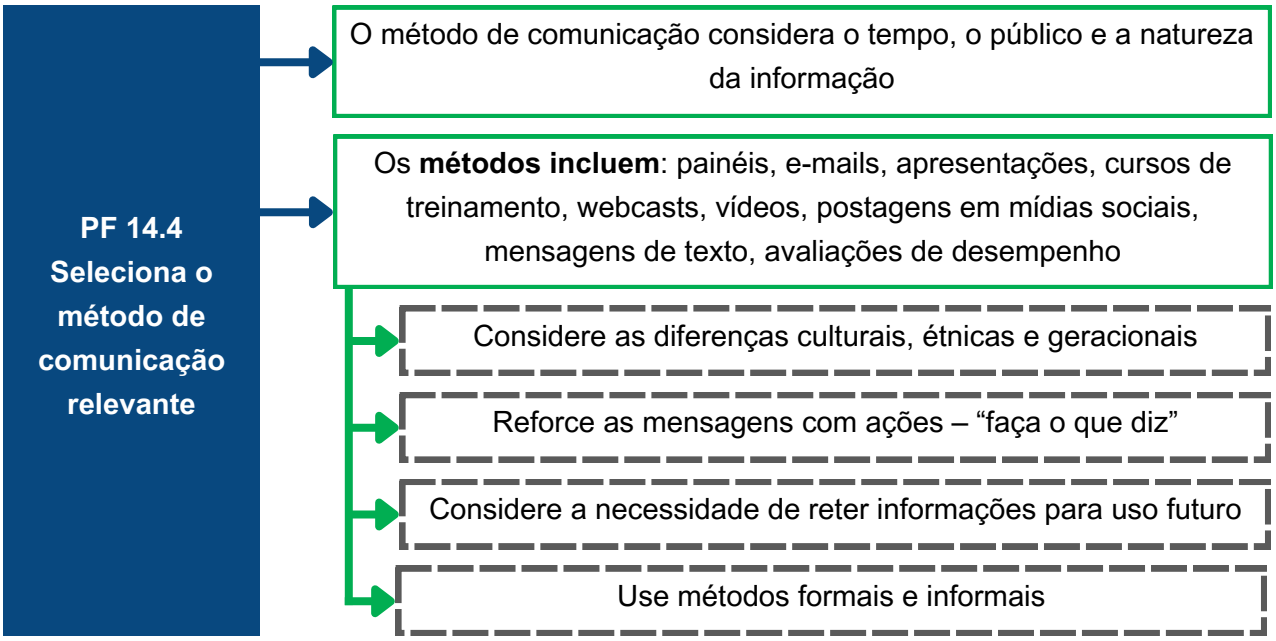
- A auditoria interna realiza auditorias periódicas da relação custo-benefício dos sistemas de informação.

- São tomadas medidas para interromper a coleta de informações que não são mais benéficas.

Princípio 14. A organização comunica internamente informações, incluindo objetivos e responsabilidades de controle interno, necessárias para apoiar o funcionamento do controle interno

Figura 17. Interpretação do Princípio 14





Comentário

A comunicação é inerente ao processamento da informação. A comunicação eficaz deve ocorrer para cima, para baixo e em toda a organização para permitir que todos os colaboradores entendam e executem suas responsabilidades de controle interno. As principais questões incluem:

- Comunicação específica e direcionada para atender às expectativas comportamentais e responsabilidades da equipe;
- Comunicação sobre as políticas e procedimentos necessários para o controle interno;
- Processos e procedimentos que se alinham e sustentam a cultura organizacional;
- Todos os colaboradores recebem mensagens claras da alta direção sobre a importância do controle interno;
- Todos os colaboradores sabem como suas atividades se relacionam com o trabalho dos outros, permitindo-lhes reconhecer problemas, determinar causas e tomar ações corretivas;
- Existem canais de comunicação abertos e disposição para ouvir, e os colaboradores acreditam que seus superiores realmente querem saber sobre os problemas e irão lidar com eles de forma eficaz; e

- Deve haver uma comunicação eficaz entre a administração e as entidades reguladoras para garantir que ambos possam cumprir suas responsabilidades de controle interno. Isso deve incluir arranjos de relatórios formais para o comitê de auditoria às entidades reguladoras para reforçar a independência da auditoria interna. Os canais de comunicação também devem existir fora das linhas normais de comunicação e o pessoal precisa entender que não haverá represálias por relatar informações relevantes.

A forma como as mensagens são comunicadas tem um impacto direto sobre o quão bem a mensagem é compreendida. Existem muitos canais diferentes disponíveis (consulte a figura 17). O momento, o público e a natureza do que está sendo comunicado devem ser considerados. Por exemplo, não seria apropriado discutir o desempenho negativo de um membro da equipe em um e-mail para todos os colaboradores. A gestão também precisa reforçar as mensagens com ações e “faça o que diz”.

Critérios para avaliar a eficácia do controle interno

A administração implementou processos para comunicar as informações necessárias para permitir que todo o pessoal entenda e execute suas responsabilidades de controle interno? Por exemplo:

- As responsabilidades de controle interno de todos os colaboradores são definidas em manuais e diretrizes.
- As políticas e procedimentos de controle interno são especificados em manuais e orientações disponíveis para todos os colaboradores.
- Os colaboradores receberam treinamento sobre a importância, relevância e benefícios de um controle interno eficaz.
- Existem controles para garantir que as principais informações sejam compartilhadas.

A administração se comunica efetivamente com as entidades reguladoras? Por exemplo:

- Existem canais de comunicação formais e informais entre a administração e as entidades reguladoras.
- A administração se comunica regularmente com as entidades reguladoras.

- Os órgãos dirigentes têm acesso direto ao pessoal da organização conforme necessário.

- O comitê de auditoria apresenta anualmente às entidades reguladoras um relatório de suas atividades.

- Cópias dos relatórios de auditoria interna estão disponíveis para as entidades reguladoras.

A administração estabeleceu canais de comunicação separados? Por exemplo:

- Existe uma linha direta de denúncia para fornecer um mecanismo à prova de falhas para permitir a comunicação confidencial quando os canais normais estiverem inoperantes ou ineficazes.

- Existe uma política de proteção a todos os denunciantes.

- A administração promove amplamente a existência da linha direta e a proteção prestada aos denunciantes.

- Existe um relatório anual sobre a eficácia da linha direta de denúncias, incluindo estatísticas que mostram a extensão do uso e as medidas tomadas para resolver os problemas levantados.

A administração seleciona métodos relevantes de comunicação para suas mensagens aos colaboradores? Por exemplo:

- A administração escolhe entre uma variedade de métodos de comunicação diferentes, dependendo do que precisa ser comunicado.

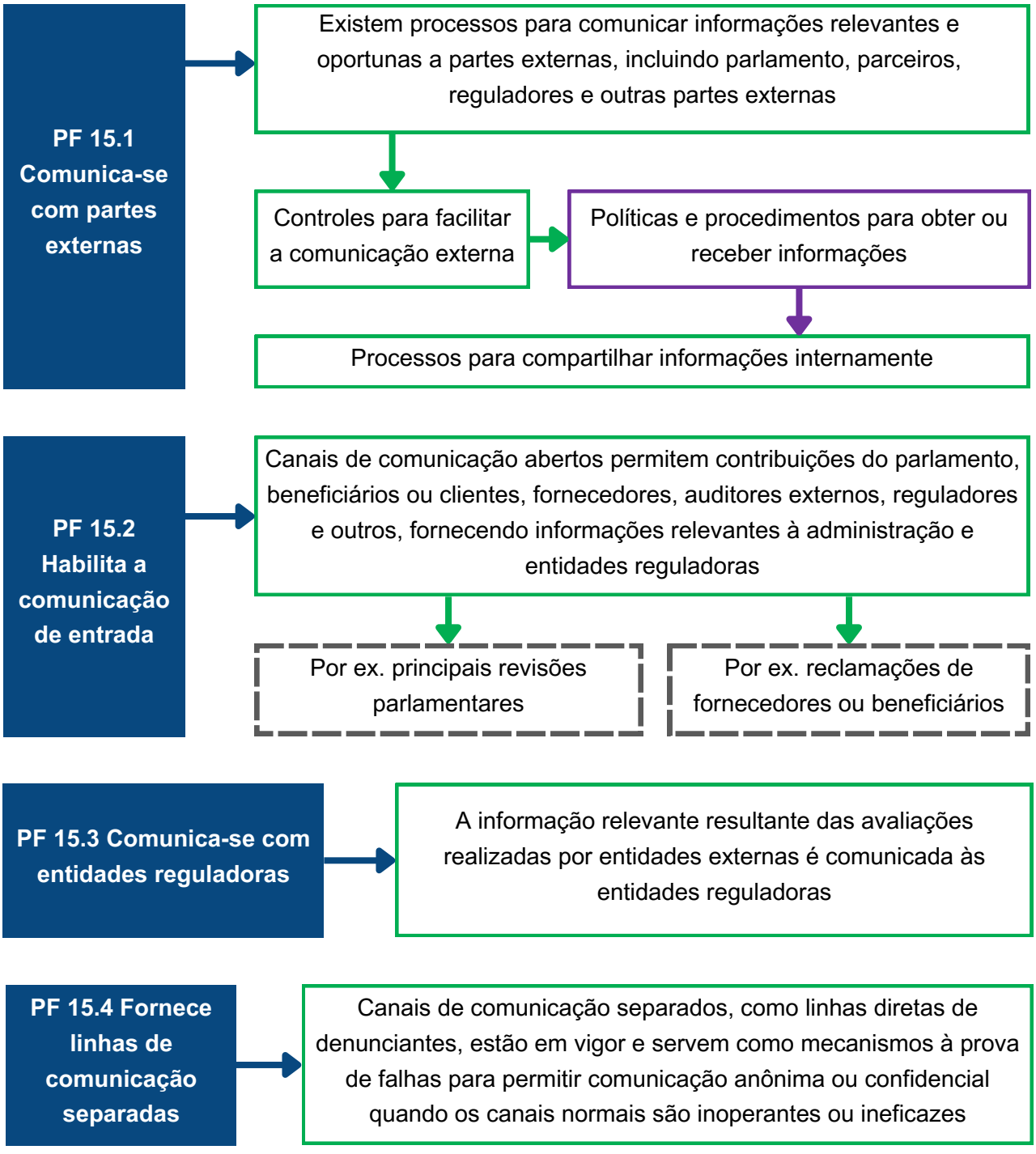
- Dependendo do nível de maturidade, tais métodos incluem painéis de gerenciamento, e-mails, apresentações, cursos de treinamento, webcasts, postagens de vídeos em mídias sociais, mensagens de texto e o processo de avaliação formal.

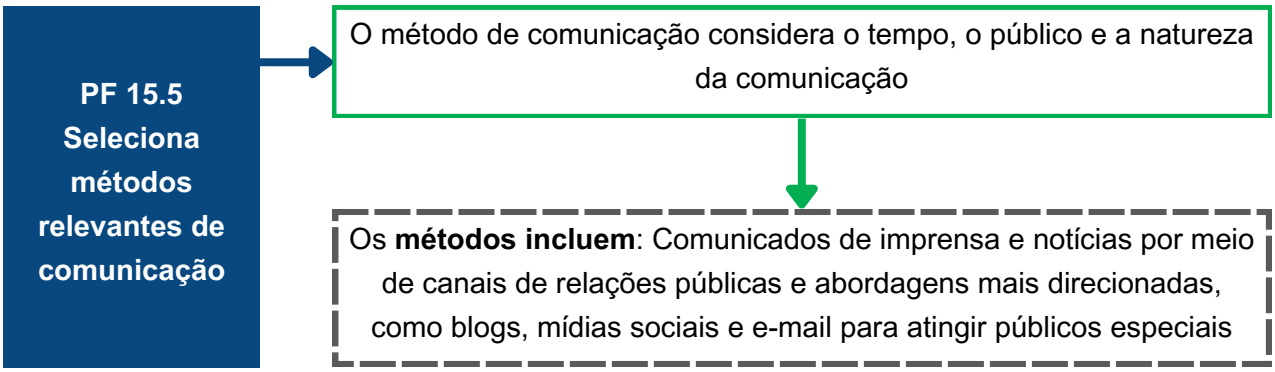
- Há reuniões regulares com todos os colaboradores sobre mudanças importantes nas funções, estrutura e objetivos operacionais da organização.

- A administração reforça as mensagens-chave com ações próprias – elas “fazem o que falam”.

Princípio 15. A organização se comunica com partes externas sobre assuntos que afetam o funcionamento do controle interno

Figura 18. Interpretação do Princípio 15





Comentário

Fortes processos de comunicação externa são uma parte crucial do controle interno. As organizações precisam implementar processos para comunicar informações relevantes e oportunas a partes externas, incluindo parlamento, parceiros, reguladores e outras partes externas. Mas a comunicação também ocorre em um sentido mais amplo, lidando com expectativas e responsabilidades de indivíduos e grupos.

A comunicação eficaz com os órgãos governamentais é particularmente importante. O estabelecimento de canais de comunicação abertos permite que partes interessadas e fornecedores forneçam feedback à organização. As organizações também precisam garantir que canais de comunicação separados, como linhas diretas de denunciantes, estejam em vigor e sirvam como mecanismos à prova de falhas para permitir comunicação anônima ou confidencial quando os canais normais estiverem inoperantes ou ineficazes.

Assim como na comunicação interna, a organização precisa usar métodos de comunicação apropriados à mensagem que está sendo entregue.

Critérios para avaliar a eficácia do controle interno

A organização se comunica de forma eficaz com as partes externas? Por exemplo:

- Existem processos em vigor para comunicar informações relevantes e oportunas a partes externas, incluindo parlamento, parceiros, reguladores e outras partes externas.
- A comunicação externa inclui relatórios regulares sobre a execução orçamental; e um relatório anual sobre as demonstrações financeiras da organização.
- Existem relatórios públicos sobre o desempenho da organização em relação aos seus objetivos operacionais.

A administração habilitou a comunicação inbound? Por exemplo:

- A Administração estabeleceu canais de comunicação abertos que permitem contribuições do parlamento, beneficiários ou clientes, fornecedores, auditores externos, reguladores e outros.

- Os relatórios dos resultados das auditorias externas da SAI são enviados ao parlamento e publicados no Diário Oficial.

- Todas as reclamações de beneficiários ou fornecedores externos são registradas para acompanhamento e ação.

A organização comunica eficazmente com as suas entidades reguladoras? Por exemplo:

- A Administração garante que as informações relevantes das avaliações realizadas por terceiros sejam comunicadas às entidades reguladoras. Estes podem incluir relatórios de reguladores e/ou auditores.

- As contas anuais, incluindo o relatório do auditor externo, são apresentadas diretamente às entidades reguladoras (ou comissão de auditoria, se existir) para consideração e revisão.

- Existe um acordo entre a administração e as entidades reguladoras sobre quais informações relacionadas às avaliações de partes externas devem ser fornecidas às entidades reguladoras e o prazo em que isso deve ser feito.

A organização estabeleceu canais de comunicação separados para permitir comunicação anônima ou confidencial quando os canais normais são ineficazes? Por exemplo:

- Existem canais de comunicação separados, como linhas diretas de denúncias, que servem como mecanismos à prova de falhas para permitir comunicação anônima ou confidencial quando os canais normais estão inoperantes ou ineficazes.

- Existe uma política de proteção a todos os denunciantes.

- A Administração promove extensivamente a existência do denunciante linha direta e a proteção oferecida aos denunciantes.

- Administração emite um relatório público sobre a eficácia da linha direta de denúncias, incluindo estatísticas mostrando a extensão do uso e as ações tomadas para resolver os problemas levantados.

A organização possui uma ampla gama de métodos de comunicação, dependendo do público que está tentando alcançar? Por exemplo:

- A administração escolhe entre uma variedade de métodos de comunicação, dependendo do que precisa ser comunicado.
- O método de comunicação considera o assunto, o momento, o público e a natureza da comunicação.
- Os métodos incluem comunicados à imprensa e notícias por meio de canais de relações públicas e abordagens mais direcionadas, como blogs, mídia social e e-mail para atingir públicos específicos.
- A organização usa mídias sociais (como Facebook e Twitter, se for o caso, para promover suas políticas).

ANEXO B5. MONITORAMENTO E AVALIAÇÃO

Este anexo centra-se na Componente 5 – Monitoramento e Avaliação que engloba a avaliação contínua dos sistemas de controlo interno e o processo de avaliações separadas.

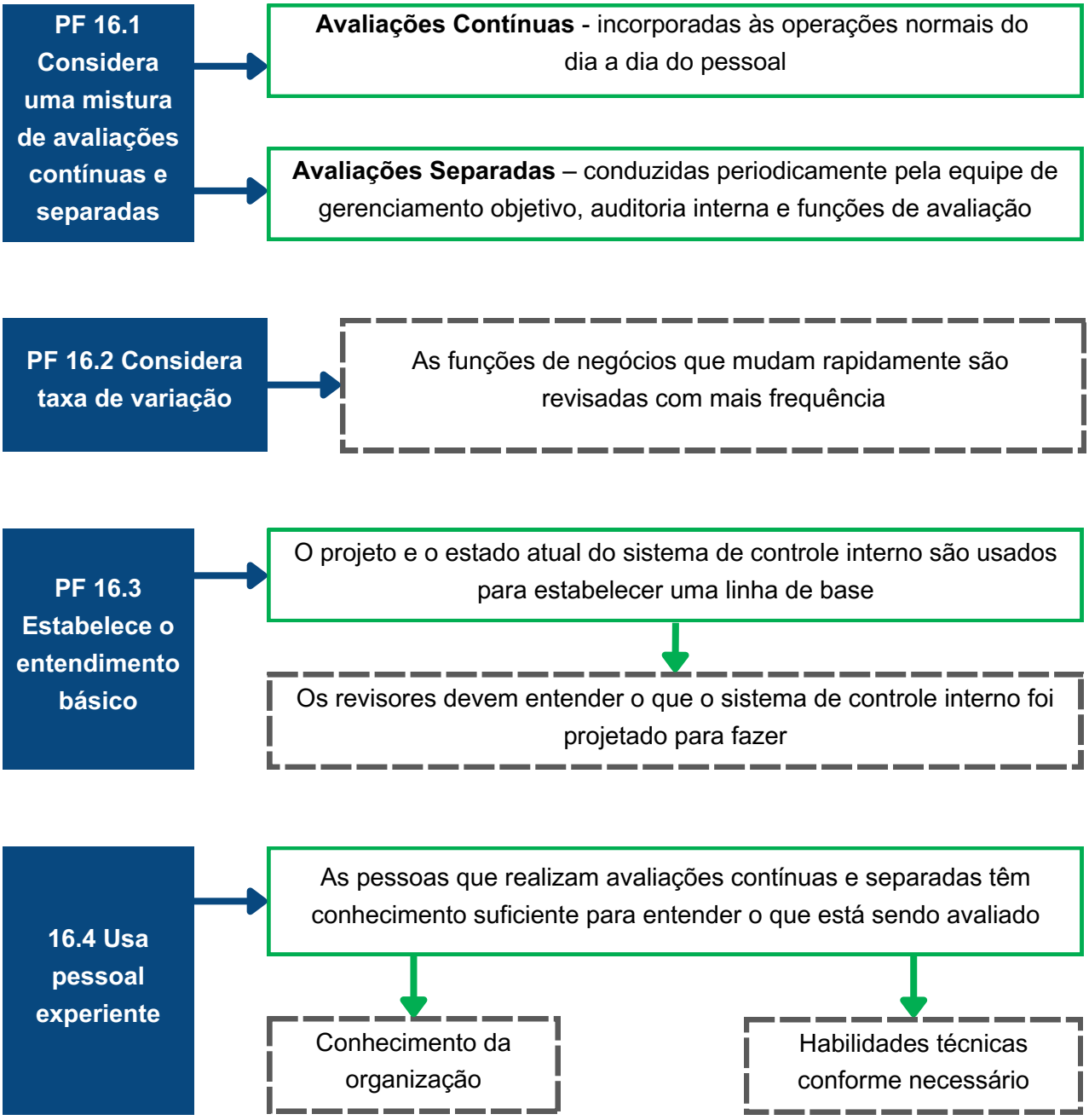
O COSO identifica **dois princípios dentro deste componente**, que estão listados na tabela abaixo.

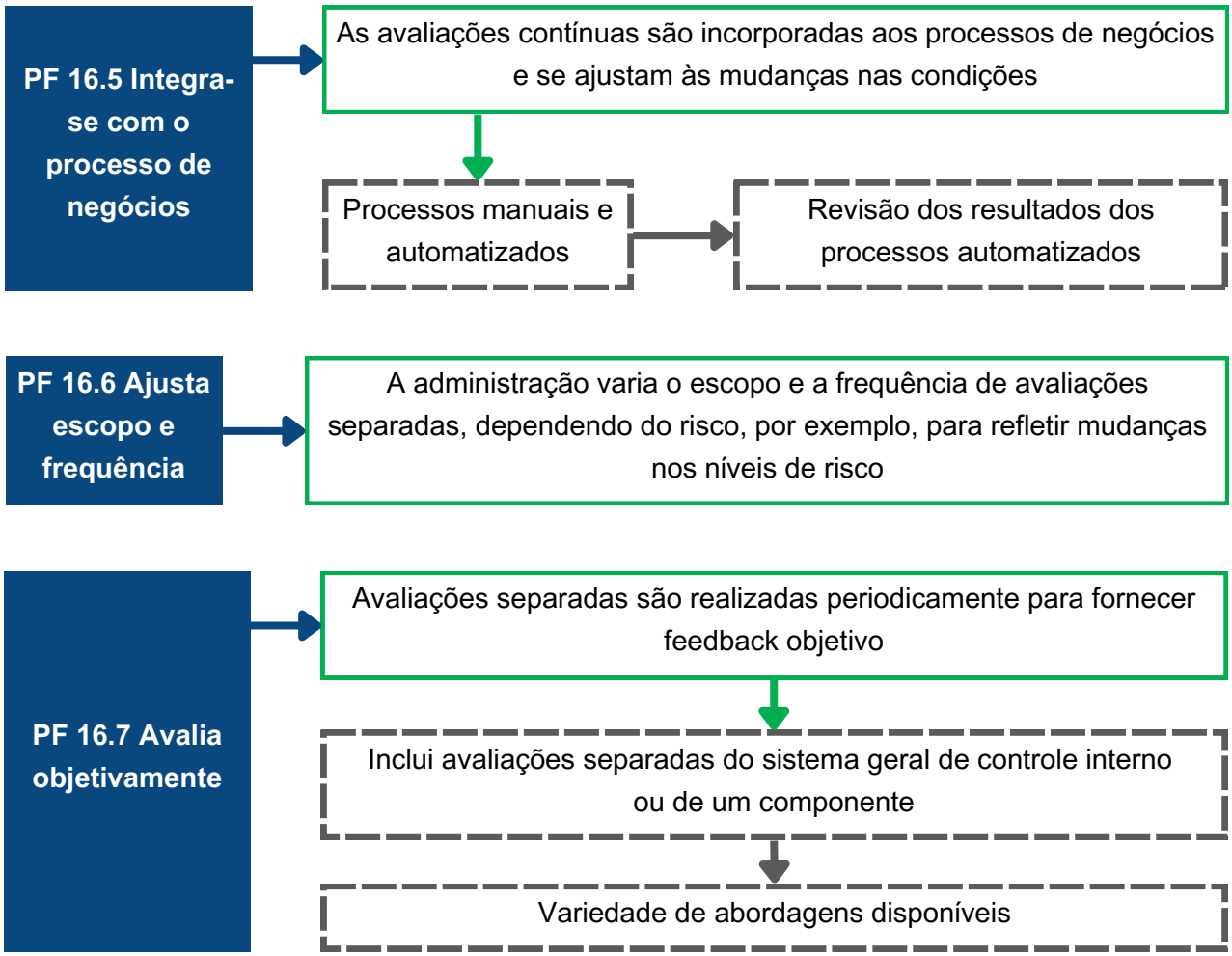
Tabela 7. Os Princípios e Pontos de Foco do Componente 5 – Monitoramento e Avaliação

Princípio	Pontos de Foco
16 A organização seleciona, desenvolve e realiza avaliações contínuas e/ou separadas para verificar se os componentes do controle interno estão presentes e funcionando.	16.1. Considera uma mistura de avaliações contínuas e separadas.
	16.2. Considera a taxa de variação.
	16.3. Estabelece entendimentos básicos.
	16.4. Usa pessoal experiente.
	16.5. Integra-se com os processos de negócios.
	16.6. Ajusta escopo e frequência.
	16.7. Avalia objetivamente.
17 A organização avalia e comunica tempestivamente as deficiências dos controles internos aos responsáveis pela adoção de ações corretivas, incluindo a alta administração e as entidades reguladoras, conforme o caso**.**	17.1. Avalia resultados.
	17.2. Comunica deficiências.
	17.3. Monitora as ações corretivas.

Princípio 16. A organização seleciona, desenvolve e realiza avaliações contínuas e/ou separadas para verificar se os componentes do controle interno estão presentes e funcionando

Figura 19. Interpretação do Princípio 16





Comentário

O controle interno não é algo que pode ser avaliado em um dia e esquecido no dia seguinte. Exige revisão contínua. Portanto, os sistemas de controle interno precisam ser monitorados – um processo que avalia a qualidade do desempenho do sistema ao longo do tempo. O monitoramento garante que o controle interno continue a operar de forma eficaz. Isso pode ser feito de duas maneiras – por meio de monitoramento contínuo ou avaliações separadas.

As atividades de **avaliação contínua** (às vezes chamadas de monitoramento) monitoram a eficácia do controle interno no curso normal das operações. Atuando como primeira linha de defesa, incluem atividades regulares de administração e supervisão, comparações, conciliações e outras ações rotineiras. O objetivo das atividades de avaliação contínua é determinar o funcionamento dos controles internos. Essas atividades devem ser construídas em operações diárias e recorrentes realizadas no curso normal da administração da organização. Eles devem ser executados em tempo real e devem reagir dinamicamente às mudanças nas condições.

Avaliações separadas incluem revisões separadas realizadas por funções de segunda linha de defesa responsáveis pela supervisão de risco, controle e conformidade. A auditoria interna também pode realizar avaliações separadas da eficácia geral dos controles internos como parte das auditorias baseadas em sistemas.

A administração precisa determinar um equilíbrio adequado entre as atividades de avaliação na primeira e segunda linhas. Unidades de negócios sujeitas a muitas avaliações separadas podem resultar em monitoramento menos contínuo, reduzindo a eficácia do controle interno. Risco e taxa de mudança são dois fatores a serem considerados ao determinar a frequência da avaliação. Processos de alto risco ou que mudam com frequência podem precisar de avaliações separadas mais frequentes ou de um nível mais alto de monitoramento contínuo.

Critérios para avaliar a eficácia do controle interno

A administração implementou um mix de avaliações contínuas e separadas? Por exemplo:

- Existe uma unidade de auditoria interna independente operando de acordo com os padrões do IIA, que incluem revisões do sistema de controle interno.
- Existe um comitê de auditoria independente que revisa a eficácia das avaliações contínuas e separadas em todas as três linhas, de acordo com as melhores práticas.
- Existe uma segunda linha de defesa robusta por parte das unidades responsáveis por: (a) assegurar a efetiva administração de riscos; e (b) conformidade com as principais políticas e padrões, incluindo padrões ambientais.

A administração considera a taxa de mudança ao determinar quais funções e processos de negócios devem ser revisados com mais frequência? Por exemplo:

- Em geral, os processos de negócios que mudam rapidamente são examinados com mais frequência do que aqueles que mudam lentamente.
- Todos os grandes projetos de capital estão sujeitos a revisões na fase de planejamento.
- Todos os principais projetos de TI estão sujeitos a revisão de acordo com a orientação do COBIT.

O projeto e o estado atual do sistema de controle interno são usados para estabelecer uma linha de base? Por exemplo:

- A administração tem uma compreensão geral do desenho e do estado atual do sistema de controle interno.
- Existe documentação completa do projeto do sistema de controle interno que é atualizada para refletir as mudanças no desempenho do sistema.
- A auditoria interna avalia e documenta a maturidade dos controles internos como parte de suas auditorias baseadas em sistemas.

A organização garante que as pessoas que realizam avaliações contínuas e separadas tenham conhecimento suficiente para entender o que está sendo avaliado? Por exemplo:

- A competência necessária para realizar avaliações contínuas e separadas é especificada nas descrições de cargo.
- Todos os colaboradores recebem treinamento básico em avaliações contínuas de controle interno.
- Todo o pessoal de auditoria interna deve ter passado em um determinado nível de competência em exames relacionados à competência.
- Colaboradores selecionados recebem treinamento adicional sobre a melhor forma de realizar avaliações separadas.

As avaliações contínuas são incorporadas aos processos de negócios e ajustadas para atender às condições de mudança? Por exemplo:

- Os gestores de primeira linha revisam os processos com base nos resultados de seu desempenho nas atividades de controle.
- A revisão dos riscos da segunda linha de defesa é realizada anualmente, a menos que as unidades de negócios estejam sujeitas a uma mudança rápida de liderança ou métodos de negócios.
- Os planos estratégico e anual de auditoria interna ajustam o cronograma de revisões dos processos de negócios para refletir as revisões da administração.

A administração varia o escopo e a frequência das avaliações separadas em função do risco? Por exemplo:

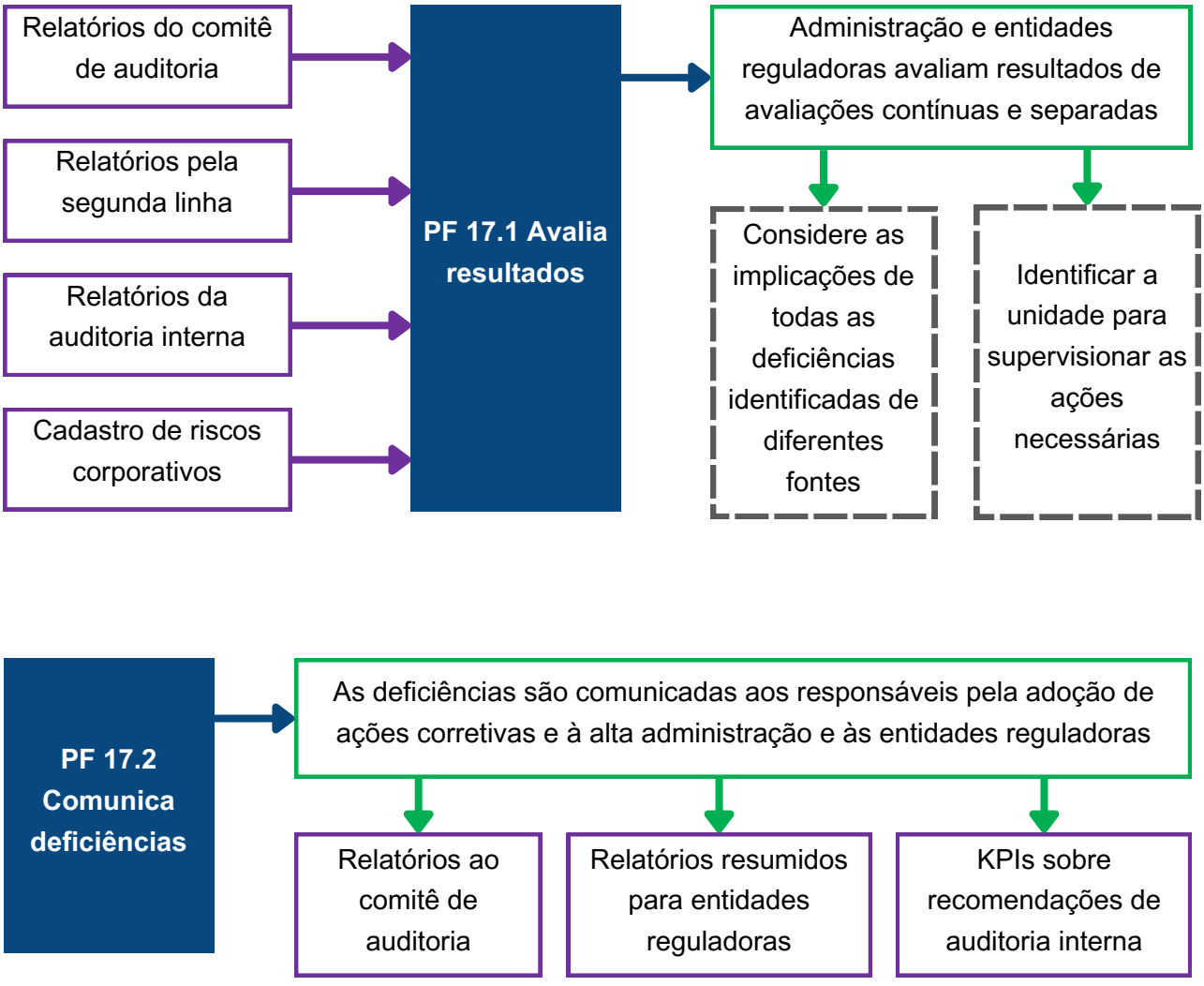
- A administração varia o escopo das avaliações separadas com base no tamanho e no tempo desde a última revisão.
- O registro de riscos corporativos identifica os altos riscos para a organização e quando as políticas e processos relacionados foram revisados pela última vez.
- Os planos estratégico e anual da auditoria interna são baseados na avaliação de riscos.

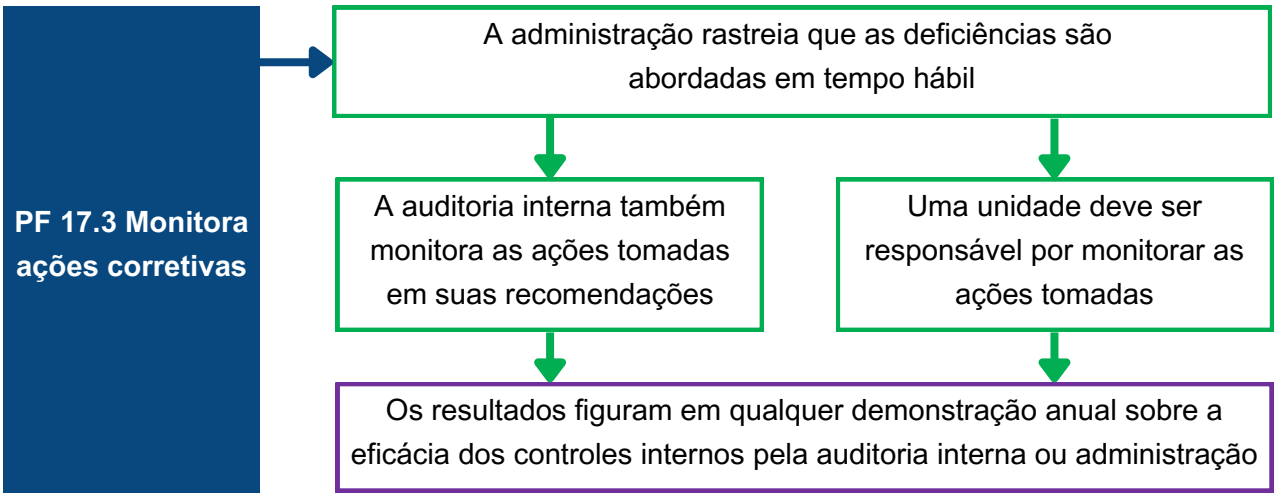
São realizadas avaliações separadas do sistema geral de controle interno ou de um dos cinco componentes principais? Por exemplo:

- A Administração revisa os componentes do sistema de controle interno de forma cíclica.
- A auditoria interna fornece uma avaliação anual da eficácia do sistema de controle interno e de cada componente do mesmo com base em seus exames durante o ano.
- Existe uma declaração anual de fiabilidade baseada na certificação da eficácia dos controlos internos por parte dos gestores individuais.

Princípio 17. A organização seleciona, avalia e comunica as deficiências de controle interno em tempo hábil às partes responsáveis pela adoção de ações corretivas, incluindo administração sênior e entidades reguladoras, conforme apropriado

Figura 20. Interpretação do Princípio 17





Comentário

As deficiências no sistema de controles internos podem surgir de várias fontes, incluindo monitoramento da administração na primeira linha de defesa, supervisão da segunda linha de defesa e avaliações da auditoria interna na terceira linha de defesa. As deficiências também podem surgir de revisões do auditor externo (geralmente a SAI) ou de um órgão de inspeção financeira[7]. Uma deficiência pode ser definida como uma condição dentro de um sistema de controle interno digna de atenção. Pode representar uma deficiência percebida, potencial ou real de um controle.

As deficiências relatadas por fontes internas e externas devem ser comunicadas às partes responsáveis por tomar ações corretivas, bem como alta administração e entidades reguladoras. Todas as deficiências devem ser sistematicamente monitoradas e ações corretivas apropriadas devem ser tomadas.

Critérios para avaliar a eficácia do controle interno

A administração e as entidades reguladoras avaliam os resultados das avaliações contínuas e isoladas dos controles internos? Por exemplo:

- Revisão administrativa de relatórios de auditoria interna sobre os resultados de auditorias baseadas em sistemas.

- Revisão administrativa de relatórios pela segunda linha de defesa.

[7] Para entender os diferentes papéis da auditoria interna, SAI e órgãos de inspeção financeira, consulte o documento conceitual PEMPAL sobre a cooperação entre auditoria do setor público e entidades de inspeção financeira www.pempal.org/knowledge-product/iacop-concept-paper-among-public-sector-auditand-financial-inspection

- Análise das causas de erros nas demonstrações financeiras identificadas pela SAI (auditoria externa).

- Revisão da administração do relatório anual do comitê de auditoria sobre a eficácia dos controles internos.

- Revisão periódica do cadastro de riscos corporativos.

As deficiências são comunicadas aos responsáveis pela adoção de ações corretivas e à alta administração e órgãos reguladores? Por exemplo:

- Todos os relatórios de auditoria interna são enviados às unidades organizacionais auditadas para revisão e recomendações de ações feitas.

- São exigidas respostas formais da unidade organizacional auditada para todas as recomendações feitas.

- A auditoria interna fornece às entidades reguladoras uma lista de todas as recomendações de auditoria pendentes (não implementadas) há mais de um ano.

A administração acompanha se as deficiências são corrigidas em tempo hábil? Por exemplo:

- Existe um ponto focal na organização responsável por monitorar relatórios/recomendações de auditoria interna e segunda linha de defesa relativos a controles internos.

- A administração reporta às entidades reguladoras as razões pelas quais as recomendações da auditoria interna estão pendentes há mais de um ano.

- A Administração fornece uma declaração anual sobre a eficácia do controle interno às suas entidades reguladoras.

ANEXO C. AVALIAÇÃO DA MATURIDADE DOS CONTROLES INTERNOS

Este anexo apresenta um quadro para avaliar a maturidade dos controlos internos a quatro níveis com base nos critérios desenvolvidos pela PEMPAL para cada princípio e nos pontos de enfoque apresentados nos Anexos B1-B5.

Para a maioria dos princípios, os níveis são cumulativos, sendo os critérios dos níveis 3 e 4 adicionais aos do nível 2. Em algumas situações, a maturidade é determinada pela medida em que os critérios foram aplicados, por exemplo, a aplicação do modelo de três linhas em PF 3.2.

Princípio 1. A organização demonstra um compromisso com a integridade e os valores éticos

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF1.1 Define o tom no topo			
O comportamento, os valores e o estilo operacional da alta administração não são conhecidos pelos colaboradores.	Os colaboradores têm conhecimento geral do comportamento e dos estilos operacionais da alta administração.	A alta administração informa a todos os colaboradores sobre seu estilo operacional e comportamento esperado. Os valores são publicados e bem compreendidos em toda a organização.	Gestores têm padrões comprovadamente elevados de comportamento pessoal. Eles “fazem o que falam”.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 1.2 Estabelece padrões de conduta			
Código mínimo ou nenhum código de conduta para os colaboradores. Nenhum padrão ético estabelecido.	Códigos-chave de conduta existem e são disponibilizados aos colaboradores. Existem políticas claras sobre fraude e corrupção, assédio sexual e proteção de denunciantes.	Os colaboradores são automaticamente lembrados dos principais padrões de comportamento esperados no âmbito de ações de formação regulares.	Colaboradores em todos os níveis têm um entendimento comum dos padrões esperados. A “forma como fazemos as coisas por aqui” é do conhecimento de todos os colaboradores.
PF1.3 Verifica a adesão aos padrões de conduta			
Nenhuma ou poucas revisões da aplicação de códigos de conduta.	Revisões administrativas dos padrões em vigor. Investigações realizadas de padrões atendidos.	As verificações fazem parte do processo anual de avaliação de desempenho.	O relatório de 360 graus inclui a avaliação da adesão aos códigos de conduta por colegas e subordinados.
PF 1.4 Aborda prontamente os desvios			
Nenhuma ou limitada ação disciplinar tomada.	Os dados são mantidos em todos os desvios dos padrões esperados. A administração tem o compromisso de agir em todos os casos de desvios dos padrões esperados.	Todos os colaboradores são notificados anualmente sobre todas as ações disciplinares tomadas contra os colaboradores.	A maioria dos colaboradores acredita que serão tomadas medidas contra todos aqueles que não cumprirem os padrões esperados.

Princípio 2. Entidades reguladoras demonstram independência da administração e exercem supervisão do desenvolvimento e desempenho de controles internos

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF2.1 Estabelecer responsabilidades de supervisão			
Os regimes de supervisão não estão definidos.	Existe um quadro legal que define claramente os órgãos de supervisão da organização.	A supervisão inclui uma comissão de auditoria independente.	Regimes de supervisão reconhecidos como atendendo aos mais altos padrões internacionais.
PF2.2 Tem acesso a habilidades relevantes			
Os regimes de supervisão não estão definidos.	Existe um processo claro de nomeação ou recrutamento de membros das entidades reguladoras. As competências necessárias e as experiências relevantes são definidas e correspondem aos objetivos da organização.	O corpo diretivo é composto por membros com várias habilidades e competências apropriadas (educação e qualificação).	O corpo diretivo é composto por membros com várias habilidades e competências apropriadas (educação e qualificação).

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF2.3 Opera de forma independente			
Os regimes de supervisão não estão definidos.	Há clara separação entre o papel decisório da administração e a função de supervisão / consultoria.	A informação necessária ao exercício da supervisão é recolhida a tempo e reportada de forma precisa e fiável	Os arranjos de supervisão foram avaliados quanto à eficiência e eficácia pela SAI.
PF2.4 Fornece supervisão do sistema de controle interno			
Os regimes de supervisão não estão definidos.	Existe um sistema estabelecido de controle interno supervisionado. A administração determina quais informações devem ser reportadas às entidades reguladoras.	Existem critérios independentes para relatar questões de controle interno às entidades reguladoras. Existe um sistema estabelecido para fornecer uma declaração sobre o status do sistema de controle interno dentro da organização.	Há uma opinião anual da auditoria interna sobre a eficácia do controle interno na organização. O comitê de auditoria fornece um relatório público sobre a eficácia do controle interno.

Princípio 3. A administração estabelece, com a supervisão dos órgãos sociais, estruturas, linhas de reporte, autoridades e responsabilidades adequadas na prossecução dos objetivos

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 3.1 Considera todas as estruturas da organização			
A estrutura organizacional não é claramente definida ou fácil de entender.	Existe uma estrutura de organização aprovada. A estrutura estabelecida é clara e de fácil compreensão.	As relações com os parceiros externos são claramente definidas pela administração. Existem contratos para prestadores de serviços terceirizados que especificam claramente as responsabilidades desses prestadores em relação ao controle interno.	As entidades reguladoras revisam regularmente a eficácia da estrutura organizacional.
PF3.2 Estabelece linhas de comunicação			
Não existe um organograma formal. Há pouca ou nenhuma consciência do modelo de três linhas.	Existem organogramas formais que especificam as linhas de subordinação. Há uma consciência básica dos papéis da primeira e da segunda linhas.	Há poucos indivíduos com responsabilidades duplas de relatórios. Todas as três linhas são bem compreendidas e totalmente implantadas.	Os resultados da terceira linha são utilizáveis e acionados.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 3.3 Define, atribui e limita autoridades e responsabilidades			
As autoridades existem, mas não foram estabelecidas para todos os níveis da organização ou não são claras.	Há uma declaração clara por escrito das autoridades delegadas de todos os colaboradores. Embora existam, eles podem não estar disponíveis para revisão por todos os colaboradores.	Os colaboradores recebem manuais ou outras orientações onde os limites de autoridade são definidos.	A auditoria interna fornece garantia sobre a clareza das autoridades e responsabilidades.

Princípio 4. A organização demonstra um compromisso para atrair, desenvolver e reter indivíduos competentes em alinhamento com os objetivos

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 4.1 Estabelece políticas e procedimentos			
As políticas de recursos humanos existem sem uma estratégia geral clara para o desenvolvimento de pessoas. Existem políticas básicas de recursos humanos que se referem principalmente a salários e subsídios.	Existe um documento de estratégia de recursos humanos que descreve os objetivos das políticas de recursos humanos da organização.	Circulares, manuais e guias identificam claramente a competência e as habilidades necessárias para o pessoal; usando, conforme necessário, estruturas de carreira, declarações de competência, descrições de cargos etc.	A estratégia e as políticas de recursos humanos são revisadas periodicamente pelas entidades reguladoras.
PF4.2 Avalia competência e aborda deficiências			
Não existe um processo formal de avaliação de desempenho.	Existe um sistema formal de avaliação de desempenho que é aplicado a todos os colaboradores.	O desempenho do pessoal é regularmente avaliado em relação aos padrões de competência esperados.	Existem testes formais exigidos das habilidades da equipe em funções críticas, como auditoria interna.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 4.3 Atrai, desenvolve e retém indivíduos			
Os colaboradores são recrutados sem uma política geral de recrutamento. As oportunidades de treinamento para os colaboradores são limitadas. Há altos níveis de rotatividade de pessoal.	Existe um mecanismo de recrutamento com regras pré-definidas e claras. Há qualificações claras exigidas para todos os colaboradores no momento do recrutamento.	Existe um plano de formação para a organização como um todo e planos de desenvolvimento pessoal para os indivíduos. A organização fornece suporte de orientação para desenvolver a equipe. Os requisitos de promoção dentro da organização estão relacionados a habilidades adicionais necessárias em níveis mais altos da organização.	Existe um mecanismo para enviar pessoal para seminários, conferências e workshops internacionais como a PEMPAL. Existem mecanismos para recompensar altos níveis de desempenho do pessoal com recompensas financeiras e não financeiras.
PF4.4 Planeja e se prepara para a sucessão			
Não há planos de sucessão em vigor	A organização identificou cargos-chave que não devem ser deixados sem preenchimento.	A organização identificou cargos em que a rotatividade de colaboradores é esperada. Existe um “plano de sucessão” para o preenchimento de cargos-chave na organização.	Existe uma política de rotação regular do pessoal para alargar a combinação de competências disponíveis. Existe um programa de orientação para ajudar a identificar futuros líderes.

Princípio 5. A organização responsabiliza os indivíduos por suas responsabilidades de controle interno na busca dos objetivos

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 5.1 Impõe a prestação de contas por meio de estruturas, autoridades e responsabilidades			
Há pouca ou nenhuma responsabilidade pela ação de controle interno	As responsabilidades são identificadas e atribuídas aos indivíduos. Existe um sistema de avaliação de desempenho que atua em diferentes níveis da organização e foca em como os gestores gerenciam sua região / escritórios / divisões / unidades.	Os colaboradores estão cientes de suas responsabilidades por meio de descrições de cargos ou outros mecanismos. As responsabilidades atendem aos objetivos de controle interno e de negócios da organização. Existem cadeias de responsabilidade bem compreendidas e a maioria dos colaboradores é responsabilizada por suas responsabilidades de controle interno.	Os objetivos individuais estão vinculados a objetivos de nível superior na estratégia ou no plano de administração. Todos os colaboradores são regularmente responsabilizados por suas responsabilidades de controle interno

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 5.2 Estabelece medidas de desempenho, incentivos e recompensas			
Existem medidas de desempenho muito limitadas.	Existe uma política para definir objetivos e KPIs **no nível da entidade**.	A política de definição de objetivos e KPIs se **estende às unidades de negócios e pessoas físicas**.	Todos os colaboradores estão ativamente envolvidos na definição de seus objetivos de desempenho e KPIs relacionados.
PF 5.3 Avalia medidas de desempenho, incentivos e recompensas por relevância contínua			
Existem medidas de desempenho muito limitadas.	A segunda linha de defesa é responsável por revisar a relevância das medidas de desempenho.	A qualidade e relevância das medidas de desempenho são regularmente avaliadas pela auditoria interna (terceira linha de defesa).	A administração atesta a relevância de suas medidas de desempenho.
PF 5.4 Considera pressões excessivas			
Existem medidas de desempenho muito limitadas.	Existe um procedimento/mecanismo formalizado para medir a carga de trabalho do pessoal que identifica situações de sobrecarga ou subcarga e mecanismos para lidar com essas disparidades.	A administração identifica os colaboradores que não estão tirando folga suficiente de suas funções. Os colaboradores que sofrem de doenças relacionadas ao estresse são identificados e são feitas alterações na carga de trabalho para reduzir esse estresse.	Existem acordos de aconselhamento do pessoal para identificar o pessoal que enfrenta pressões indevidas.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF5.5 Avalia o desempenho e recompensa ou disciplina os indivíduos			
Não existe um sistema formal de avaliação de desempenho.	Existe um sistema formal de avaliação de desempenho que é aplicado a todos os colaboradores.	O sistema de avaliação resulta em relatórios formais de desempenho. Existe consistência entre o nível de funções assumidas e as recompensas fornecidas.	A avaliação de desempenho resulta na recompensa positiva e negativa (financeira e não financeira) do pessoal.

Princípio 6. A organização especifica os objetivos com clareza suficiente para permitir a identificação e avaliação dos riscos relacionados aos objetivos

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 6.1 Objetivos das operações			
Os objetivos operacionais existem em leis e documentos de política relacionados, mas não são capturados dentro de uma estratégia geral para a organização.	Existe uma estratégia de alto nível para a organização que contém os objetivos da organização como um todo. Os objetivos organizacionais refletem as escolhas da administração e do nível político sobre a melhor forma de responder aos desafios das políticas.	A estratégia de alto nível é suportada por metas e KPIs. Cada unidade de negócios da organização define objetivos anuais com metas e KPIs relacionados.	Os objetivos de operações formam a base para definir o orçamento da organização. Há uma declaração clara do apetite de risco geral da organização. Os níveis de tolerância ao risco são identificados para todos os objetivos principais e medidos por meio de KPIs relevantes.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 6.2 Objetivos de relatórios externos			
Os relatórios externos são ad hoc e não estruturados.	A organização mantém registros de receitas e despesas em relação ao orçamento alocado e relata o resultado do orçamento ao ministério das finanças. Os relatórios de desempenho são fornecidos quando solicitados pelas entidades reguladoras.	A organização é obrigada a preparar demonstrações financeiras anuais de acordo com as normas contábeis adotadas para a organização como um todo. Existe um sistema para a preparação de relatórios anuais sobre o desempenho da organização em relação aos seus objetivos declarados.	Existe um sistema de contabilidade automatizado que oferece suporte à preparação precisa de contas para refletir as transações subjacentes a um nível aceitável de materialidade
PF 6.3 Objetivos do relatório interno			
Há relatórios internos limitados.	Os relatórios internos são elaborados pelas unidades da organização quando o consideram adequado.	Os relatórios internos são preparados com um nível adequado de precisão e refletem as transações subjacentes.	A alta administração decide qual nível de reporte interno é apropriado para diferentes aspectos do orçamento e da administração financeira.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 6.4 Objetivos de compliance			
Há uma consciência limitada dos objetivos de compliance.	Existe uma política que explica como os gestores devem estabelecer objetivos para cumprir os padrões de todo o governo. Os objetivos de compliance podem ser amplos e incluir questões ambientais, a necessidade de regulamentação de concorrência e segurança e políticas fundamentais de pessoal, como taxas mínimas de pagamento e assédio.	Os objetivos de compliance estão incluídos na estratégia de alto nível da organização. A organização atende a todos os principais objetivos de compliance.	Há um alto nível de conscientização na organização sobre a importância dos objetivos de compliance.

Princípio 7. A organização identifica os riscos para a realização de seus objetivos em toda a organização e analisa os riscos como base para determinar como os riscos devem ser gerenciados

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 7.1 Inclui organização e estruturas principais			
Não existe uma avaliação formal de riscos, portanto a administração reage aos riscos e oportunidades à medida que surgem.	Há um requisito para processos formais de avaliação de riscos em toda a organização. A maioria das unidades organizacionais realiza algum tipo de avaliação de risco.	Existem registros de risco separados para escritórios regionais e centrais. Existem registos de risco separados para unidades organizacionais que funcionam como agências autónomas sem fins lucrativos que cobram pelos seus serviços ou produtos.	Existem registros de riscos separados para cada unidade operacional e um registro de riscos corporativos para os principais riscos enfrentados pela organização como um todo.
PF 7.2 Analisa fatores internos e externos			
Não há nenhuma avaliação de risco formal em vigor.	Existe uma política formal de avaliação de riscos que explica como identificar e avaliar o impacto de eventos internos e externos.	Os colaboradores recebem exemplos dos tipos de eventos internos e externos que podem levar a riscos e oportunidades.	Os colaboradores são treinados em como realizar uma avaliação de risco formal.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 7.3 Envolve níveis adequados de administração			
A alta administração não pode estar envolvida na resposta aos riscos decorrentes.	As avaliações de risco podem envolver colaboradores de diferentes níveis em algumas unidades organizacionais.	Na maioria das unidades, colaboradores de diferentes níveis normalmente realizam reuniões separadas de avaliação de risco.	As avaliações de risco são sempre realizadas em reuniões envolvendo colaboradores de todos os níveis.
PF 7.4 Estima a significância dos riscos identificados			
A importância dos riscos decorrentes pode não ser totalmente compreendida.	O registro de riscos contém avaliações da **probabilidade** e **impacto** de todos os riscos identificados.	A **velocidade** do risco também é considerada e medida durante o processo de avaliação de risco.	Existe um sistema comum para pontuar riscos em toda a organização para determinar os riscos mais altos enfrentados pela organização, medindo probabilidade, impacto e velocidade.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 7.5 Determina como responder ao risco			
A administração reage aos riscos e oportunidades à medida que surgem.	A política de avaliação de risco fornece quatro possíveis respostas ao risco - evitar, transferir (compartilhar), aceitar ou reduzir (controlar) o risco.	O registro de risco inclui a resposta de risco acordada e referências a atividades de controle, conforme apropriado.	A administração garante que as respostas aos riscos sejam econômicas, fazendo uso apropriado de todas as quatro respostas aos riscos.

Princípio 8. A organização considera o potencial de fraude na avaliação dos riscos para o alcance dos objetivos

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 8.1 Considera vários tipos de fraude			
Há uma compreensão mínima das causas da fraude e da corrupção.	Existe uma política antifraude e anticorrupção que explica aos colaboradores as diferentes formas pelas quais a fraude e a corrupção podem ocorrer, por exemplo, roubo, engano, uso indevido de ativos, relatórios fraudulentos, descumprimento de controles da administração e atos ilegais.	Todos os colaboradores recebem treinamento básico sobre conscientização sobre fraude e corrupção.	Casos reais de fraude e corrupção identificados são relatados a todos os colaboradores para levantar consciência de como a fraude pode ser cometida.
8.2 Avalia incentivos e pressões			
Existem avaliações limitadas dos incentivos e pressões para cometer fraudes.	Há adequada segregação de funções para garantir que os gestores não possam tomar decisões por conta própria: o princípio dos quatro olhos é seguido.	Há verificações periódicas de conflitos de interesse na tomada de decisões.	Todos os colaboradores em cargos gerenciais são obrigados a fornecer uma declaração de sua situação financeira a cada ano.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 8.3 Avalia oportunidades			
Há avaliações limitadas das oportunidades de cometer fraudes.	A administração inclui avaliações de oportunidades de fraude durante os processos de avaliação de risco.	Os fatores que levam à alta rotatividade de colaboradores em funções-chave foram identificados. A administração identifica posições financeiras de alto risco para níveis adicionais de revisão.	A administração divulga todos os casos de fraude e corrupção para aumentar o medo de detecção de fraudes ou atos corruptos.
PF 8.4 Avalia atitudes e racionalizações			
Há consideração limitada de atitudes e racionalizações.	Todos os colaboradores tiveram um nível mínimo de treinamento em conscientização sobre fraude e corrupção.	O registo de riscos inclui áreas de maior risco de fraude e corrupção.	Há verificações periódicas de comportamento pessoal. Existe um comitê interno sobre práticas antifraude. A auditoria interna realiza revisões de terceira linha dos riscos de fraude e corrupção.

Princípio 9. A organização identifica e avalia as mudanças que podem impactar significativamente o sistema de controle interno

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 9.1 Avalia mudanças no ambiente externo			
Há uma consideração limitada de grandes mudanças no ambiente externo.	A administração considera mudanças decorrentes da disponibilidade de recursos (redução do quadro de colaboradores ou outros recursos orçamentários). A administração considera mudanças no ambiente externo fora do controle da organização, como impactos climáticos severos.	A administração considera mudanças na (a) direção política (governo); (b) as direções econômicas / políticas / geográficas globais; (c) o quadro regulamentar; (d) grande reestruturação do setor público – fusão de ministérios/agências ; e (e) mudanças contínuas ou esperadas nas práticas da administração pública ou GFP/PIC.	Existe uma unidade dentro da organização que é responsável por monitorar a mudança.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 9.2 Avalia mudanças no modelo de negócios			
Há uma consideração limitada de grandes mudanças no modelo de negócios.	A administração considera grandes projetos de mudança que resultam em mudanças nas principais estruturas, funções, papéis, serviços e produtos entregues. Administração considera mudanças em novas tecnologias disruptivas, incluindo dados móveis e seu impacto nos processos internos e controle interno.	Existem processos claros para lidar com tecnologias de informação e comunicação/riscos de segurança cibernética e disponibilidade operacional por meio de planejamento de continuidade de negócios e/ou planejamento de recuperação de desastres. A administração considera a capacidade de pessoal relevante para novas funções e objetivos.	Existe uma unidade dentro da organização que é responsável por monitorar a mudança.
PF 9.3 Avalia mudanças na liderança			
Há consideração limitada de mudanças na liderança.	A administração considera o impacto de novos gestores com uma nova visão de PIC e diferentes atitudes de controle.	A administração considera o impacto de altos níveis de rotatividade nos cargos de administração de forma geral.	Existe uma unidade dentro da organização que é responsável por monitorar a mudança.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
		Existem trabalhos específicos que possuem acordos formais de transferência para garantir que as informações sobre as principais atividades de controle sejam passadas de um gestor para outro.	

Princípio 10. A organização desenvolve atividades de controle que contribuam para a mitigação dos riscos para o alcance dos objetivos aos níveis de responsabilidade

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 10.1 Integra-se com a avaliação de risco			
Não há avaliação de risco formal para integrar com controles	A maioria dos registros de riscos inclui algumas referências às atividades de controle que visam reduzir os riscos inerentes a um nível aceitável.	Existem referências às atividades de controle em todos os registros de riscos.	Existe um registro de riscos corporativos que identifica os principais riscos enfrentados pela organização e as principais atividades de controle implementadas para lidar com esses riscos.
PF 10.2 Considera fatores específicos da organização			
Há pouca consideração de fatores organizacionais, como os níveis de descentralização e automação de TI ao projetar controles.	A organização tem um entendimento básico da primeira e segunda linhas ao projetar atividades de controle.	A organização entende e aplica o conceito das três linhas ao projetar suas atividades de controle.	A organização utiliza as três linhas para estabelecer controles efetivos sobre as atividades descentralizadas: há um conjunto comum de orientações para gestores de escritórios regionais sobre os papéis da segunda e terceira linhas em relação às atividades regionais.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 10.3 Determina os processos de negócios relevantes			
As atividades de controle são definidas e aplicadas de maneira padronizada no setor público, independentemente do processo de negócios.	Existe um entendimento básico de quais processos de negócios requerem atividades de controle. Isso inclui políticas que especificam quais tipos de contratos exigem licitações competitivas e processos críticos para a preparação de demonstrações financeiras precisas.	Os objetivos dos processos de negócios abrangem **integridade** (que todas as transações sejam processadas), **precisão** (que as transações sejam avaliadas e registradas corretamente) e **validade** (que as transações representem despesas ou receitas legítimas da organização e tenham sido devidamente autorizadas de acordo com o orçamento).	Há uma compreensão completa de quais processos de negócios requerem atividades de controle.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 10.4 Avalia uma combinação de tipos de atividades de controle			
A administração não avalia o mix de atividades de controle.	Há uma compreensão clara das diferenças entre controles preventivos e de detecção e uma abordagem equilibrada para o uso de cada tipo de controle.	A administração faz pleno uso de diferentes tipos de controles, por ex. reconciliações, controles físicos, autorizações e aprovações e verificações de terceiros. Tentativas básicas são feitas para reduzir custos limitando as verificações de transações abaixo de um determinado valor financeiro.	A administração avalia o custo-benefício de diferentes atividades de controle antes de determinar quais atividades de controle implementar.
PF 10.5 Considera em que nível as atividades de controle são aplicadas			
A administração não considera o nível das atividades de controle.	Existem requisitos separados para atividades de controle nos níveis de transação e supervisão na maioria dos processos de negócios.	Existem requisitos separados para atividades de controle nos níveis de transação e supervisão em todos os processos de negócios.	Sempre que possível, a administração concentra os principais controles no nível de supervisão.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 10.6 Aborda a segregação de funções			
Há uma segregação limitada de funções.	A administração identificou quatro funções principais que devem ser segregadas – (1) autorizar gastos, (2) certificar bens recebidos e aprovar pagamentos, (3) efetuar pagamentos e (4) registrar transações.	Há verificações adicionais por uma unidade de supervisão de segunda linha quando a segregação não é prática devido ao tamanho da unidade de negócios.	A auditoria interna revisa a adequação da segregação de funções como parte da terceira linha de defesa.

Princípio 11. A organização seleciona e desenvolve atividades gerais de controle sobre a tecnologia para apoiar o alcance dos objetivos

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 11.1 Determina a dependência entre o uso de tecnologia em processos de negócios e controles gerais de tecnologia			
Não há avaliação da dependência de TI.	Existe uma política de TI separada que identifica todos os principais elementos de TI em uso na organização. A política inclui consideração de tecnologia de cliente/servidor, armazenamento de dados baseado em nuvem, computação de usuário final, dispositivos móveis e sistemas operacionais.	A administração entende e determina a dependência e ligação entre atividades de controles automatizados de processos de negócios e controles gerais de tecnologia.	Administração utiliza a estrutura COBIT 5 para a governança e administração de sistemas e processos de TI em toda a entidade.
PF 11.2 Estabelece atividades relevantes de controle de infraestrutura de tecnologia			
Existem controles limitados sobre a infraestrutura de tecnologia.	A administração seleciona e desenvolve atividades de controle sobre a infraestrutura tecnológica, que visam garantir a	Existem procedimentos diários de backup e recuperação claramente definidos para todos os dados importantes da organização.	Existem procedimentos como geradores de energia de backup para garantir um alto nível de disponibilidade dos

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
	integridade, precisão e disponibilidade do processamento tecnológico.		sistemas corporativos de TI.

PF 11.3 Estabelece atividades relevantes de controle do processo de administração de segurança

Existem controles mínimos de segurança de TI.	Existem atividades básicas de controle para restringir os direitos de acesso a usuários autorizados de acordo com suas responsabilidades de trabalho, usando controles físicos sobre o acesso a escritórios com infraestrutura de TI e senhas de usuário para acessar sistemas de TI	Existem fortes controles de segurança de TI que incluem alterações regulares para acessar senhas e o uso de fortes convenções de nomenclatura de senha.	Existem limitações estritas e automáticas de acesso dos utilizadores apenas às aplicações indispensáveis ao desempenho das funções.

PF 11.4 Estabelece atividades relevantes de controle de processo de aquisição, desenvolvimento e manutenção de tecnologia

Não há procedimentos especiais para controlar os processos de aquisição e manutenção de TI.	Uma unidade de TI especializada é responsável pela aquisição, desenvolvimento e manutenção dos processos de TI.	Um comitê de alto nível supervisiona os desenvolvimentos de TI para a organização como um todo.	A organização segue a estrutura COBIT 5 para todas as suas aquisições e descartes de TI.

Princípio 12. A organização implementa atividades de controle por meio de políticas que estabelecem o que é esperado e em procedimentos que colocam as políticas em prática

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz

PF 12.1 Estabelece políticas e procedimentos para apoiar a implantação das diretrizes da administração

Não há políticas e procedimentos claros relacionados às atividades de controle.	Para a maioria dos controles, existe (a) um conjunto de políticas que identificam o que deve ser feito em termos de controle e (b) a documentação dos procedimentos (etapas) a serem seguidos para implementar a política.	A política e os procedimentos são documentados para todos os controles.	Há treinamento obrigatório para a equipe na implementação de controles-chave.

PF 12.2 Estabelece responsabilidade e prestação de contas pela execução de políticas e procedimentos

Não há alocação clara de responsabilidade para as atividades de controle.	A responsabilidade pela maioria dos elementos do processo de controle é atribuída a indivíduos nomeados.	Todos os elementos do processo de controle são alocados para indivíduos nomeados.	Gestores e colaboradores recebem treinamento sobre a importância de implementar controles de forma ponderada, consciente e consistente.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 12.3 Executa em tempo hábil			
Não há padrões para a pontualidade das ações de controle.	Existem padrões predefinidos para o tempo necessário para realizar atividades críticas de controle, como o tempo para processar pagamentos ou as datas em que as reconciliações bancárias devem ser concluídas. No entanto, os padrões nem sempre são seguidos.	Existe um alto nível de cumprimento dos padrões de tempestividade das atividades de controle.	Existem relatórios regulares para supervisores e gestores sobre a pontualidade do processamento de negócios.
PF 12.4 Toma ação corretiva			
A ação corretiva nem sempre pode ser tomada.	Existem procedimentos para tomar ações corretivas e são seguidos na maioria das vezes.	Procedimentos para ação corretiva são sempre executados. Os supervisores de nível superior devem autorizar pessoalmente o processamento de todas as transações que foram rejeitadas pelas verificações de validação do sistema.	Existem relatórios regulares para supervisores e gestores sobre áreas onde não foram tomadas ações corretivas.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 12.5 Executa usando pessoal competente			
Não há garantia de que pessoal competente será designado para as atividades de controle.	O nível de competência e autoridade exigido para realizar cada atividade de controle é claramente definido e normalmente aplicado.	Gestores e colaboradores estão cientes da competência e autoridade necessárias para realizar controles de forma eficaz.	Despesas acima de limites financeiros predeterminados devem ser autorizadas por colaboradores mais graduados.
PF 12.6 Reavalia políticas e procedimentos			
Políticas e procedimentos não podem ser reavaliados	A administração revisa a relevância das atividades de controle, mas isso pode não ser feito regularmente.	Há um cronograma claro para revisões da relevância contínua das atividades de controle. A alta administração acorda com a auditoria interna a frequência com que realizam auditorias baseadas em sistemas dos principais processos de negócios.	Todas as delegações financeiras têm uma cláusula de caducidade que especifica a data em que devem ser revisadas para determinar sua relevância contínua.

Princípio 13. A organização obtém ou gera e usa informações relevantes e de qualidade para apoiar o funcionamento do controle interno

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 13.1 Identifica requisitos de informação			
Os requisitos de informação do controle interno não são claros.	As necessidades de informação dos controles mais importantes são especificadas em manuais e procedimentos internos. O processo de comunicação de fornecer e compartilhar informações funciona na maioria das vezes.	As necessidades de informação de todos os controles são especificadas em manuais e procedimentos internos. O processo de comunicação funciona muito bem.	Pessoal individual recebe a responsabilidade de (a) definir as necessidades de informação e (b) gerar os dados para atender a essas necessidades.
PF 13.2 Captura fontes internas e externas de dados			
O processo de captura de fontes internas e externas de dados não funciona bem.	A organização possui sistemas básicos para coleta de dados internos (e-mails, relatórios financeiros e orçamentos) e externos (debates parlamentares e cobertura da imprensa).	A organização possui sistemas mais sofisticados para a coleta de dados internos e externos. Existe um sistema único para processar todos os dados contábeis da organização.	O processo de captura e comunicação de informações é altamente automatizado.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 13.3 Processa dados relevantes em informações			
Há processamento limitado de dados em informações. Somente dados brutos são comunicados.	A organização possui sistemas de informação para processar dados críticos em informações utilizáveis para os gestores. Eles existem para alguns, mas não para todos os processos de negócios.	A organização possui sistemas de informação para processar dados críticos em informações utilizáveis por gestores para todos os processos de negócios.	Dados que não atendam aos critérios de precisão não são incluídos nos relatórios da administração.
PF 13.4 Mantém a qualidade durante todo o processamento			
Existem verificações limitadas sobre a qualidade do processamento.	Os sistemas mais importantes são projetados para produzir informações oportunas, atuais, precisas, completas, acessíveis, protegidas, verificadas e retidas.	Todos os sistemas são projetados para produzir informações oportunas, atuais, precisas, completas, acessíveis, protegidas, verificadas e retidas.	Todos os sistemas de entrada de dados financeiros têm maneiras de validar os dados originais (por exemplo, por meio de digitação dupla, aprovação do supervisor etc.) antes que os dados sejam aceitos para processamento.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 13.5 Considera custos e benefícios			
Não há consideração dos custos e benefícios da coleta de informações.	Para os principais processos de negócios, a administração analisa a natureza, quantidade e precisão das informações comunicadas e verifica se o custo de coleta das informações é compatível com os benefícios obtidos.	A administração revisa custos e benefícios para todos os processos de negócios. A organização identifica o custo de produzir os principais relatórios sobre a eficácia dos controles internos, incluindo os custos diretos do exame de auditoria interna.	A auditoria interna realiza auditorias periódicas do custo-benefício dos sistemas de informação. Ação é tomada para parar de coletar informações que não são mais benéficas.

Princípio 14. A organização comunica internamente informações, incluindo objetivos e responsabilidades de controle interno, necessárias para apoiar o funcionamento do controle interno

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz

PF 14.1 Comunica informações de controle interno

Existem poucos processos formais em vigor para garantir que a equipe entenda suas responsabilidades de controle interno.	As responsabilidades de controle interno de todos os colaboradores são definidas em manuais e diretrizes. As políticas e procedimentos de controle interno são especificados em manuais e orientações disponíveis para todos os colaboradores.	Os colaboradores foram treinados sobre a importância, relevância e benefícios de um controle interno eficaz.	Existem controles para garantir que as principais informações sejam compartilhadas.

PF 14.2 Comunica-se com entidades reguladoras

Existe uma comunicação limitada sobre controles internos entre a administração e as entidades reguladoras.	Existem canais formais e informais de comunicação entre a administração e as entidades reguladoras. A administração utiliza principalmente canais de comunicação formais.	A administração utiliza canais de comunicação formais e informais. As entidades reguladoras têm acesso direto ao pessoal da organização conforme necessário.	A comissão de auditoria apresenta anualmente um relatório das suas atividades às entidades reguladoras. Cópias dos relatórios de auditoria interna são disponibilizadas às entidades reguladoras.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 14.3 Fornece linhas de comunicação separadas			
Não há linhas de comunicação separadas.	Existe uma linha direta de denúncia para fornecer um mecanismo à prova de falhas para permitir a comunicação confidencial quando os canais normais estiverem inoperantes ou ineficazes.	Existe uma política para a proteção de todos os denunciantes. A administração promove amplamente a existência da linha direta e a proteção prestada aos denunciantes.	Há um relatório anual sobre a eficácia da linha direta de denúncias, incluindo estatísticas que mostram a extensão do uso e as medidas tomadas para resolver os problemas levantados.
PF 14.4 Seleciona o método de comunicação relevante			
A organização usa um número limitado de formas tradicionais de comunicação com o pessoal.	Administração escolhe entre uma variedade de métodos tradicionais de comunicação, dependendo do que precisa ser comunicado. Esses métodos incluem e-mails, apresentações, cursos de treinamento e o processo de avaliação formal.	A administração tem mais formas de se comunicar com a equipe, por exemplo: painéis de administração, webcasts, vídeos, postagens em redes sociais e mensagens de texto. Há reuniões regulares com todos os colaboradores sobre mudanças importantes nas funções, estrutura e objetivos operacionais da organização.	A administração reforça as mensagens-chave com suas próprias ações – elas “fazem o que falam”.

Princípio 15. A organização se comunica com partes externas sobre assuntos que afetam o funcionamento do controle interno

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 15.1 Comunica-se com partes externas			
Há comunicação limitada com partes externas	Existem processos em vigor para comunicar informações relevantes e oportunas a partes externas, incluindo parlamento, parceiros, reguladores e outras partes externas.	A comunicação externa inclui relatórios regulares sobre a execução orçamental e um relatório anual sobre as demonstrações financeiras da organização.	Existem relatórios públicos sobre o desempenho da organização em relação aos seus objetivos operacionais.
PF 15.2 Habilita a comunicação de entrada			
A administração não incentiva a comunicação receptiva.	A administração estabeleceu canais de comunicação abertos que permitem contribuições do parlamento, beneficiários ou clientes, fornecedores, auditores externos, reguladores e outros.	Os relatórios dos resultados das auditorias externas da SAI são enviados ao parlamento e publicados no Diário Oficial.	Todas as reclamações de beneficiários ou fornecedores externos são registradas para acompanhamento e ação.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 15.3 Comunica-se com entidades reguladoras			
Há comunicação limitada com as entidades reguladoras sobre os resultados das avaliações por partes externas.	A administração assegura que a informação relevante das avaliações realizadas por entidades externas é comunicada às entidades reguladoras. Estes podem incluir relatórios de reguladores e/ou auditores.	As contas anuais, incluindo o relatório do auditor externo, são apresentadas diretamente às entidades reguladoras (ou comissão de auditoria, caso exista) para apreciação e revisão.	Existe acordo entre a administração e as entidades reguladoras sobre quais informações relacionadas às avaliações de partes externas devem ser fornecidas às entidades reguladoras e o prazo para isso.
PF 15.4 Fornece linhas de comunicação separadas			
Não há linhas de comunicação separadas.	Canais de comunicação separados, como linhas diretas de denunciantes, estão em vigor e servem como mecanismos à prova de falhas para permitir comunicação anônima ou confidencial quando os canais normais são inoperantes ou ineficazes.	Existe uma política para a proteção de todos os denunciantes. A administração promove extensivamente a existência da linha direta de denúncias e a proteção prestada aos delatores.	A administração emite um relatório público sobre a eficácia do canal de denúncias, incluindo estatísticas que mostram a extensão do uso e as ações tomadas para resolver os problemas levantados.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 15.5 Seleciona métodos relevantes de comunicação			
A organização tem métodos limitados de comunicação externa.	A administração escolhe entre uma variedade de métodos tradicionais de comunicação dependendo do que precisa ser comunicado. O método de comunicação considera o assunto, o momento, o público e a natureza da comunicação. Os métodos incluem comunicados à imprensa e notícias por meio de canais de relações públicas.	A administração tem abordagens mais direcionadas como blogs, redes sociais e e-mail para atingir públicos específicos.	A organização usa redes sociais como Facebook e Twitter para promover suas políticas.

Princípio 16. A organização seleciona, desenvolve e realiza avaliações contínuas e/ou separadas para verificar se os componentes do controle interno estão presentes e funcionando

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 16.1 Considera uma mistura de avaliações contínuas e separadas			
Existem avaliações limitadas em andamento e separadas.	Existe uma unidade de auditoria interna independente operando de acordo com os padrões do IIA, que incluem revisões do sistema de controle interno.	Há um comitê de auditoria independente que revisa a eficácia das avaliações contínuas e separadas em todas as três linhas de defesa, de acordo com as melhores práticas.	Existe uma segunda linha de defesa robusta por parte das unidades responsáveis por: (a) assegurar a efetiva administração dos riscos; e (b) conformidade com as principais políticas e padrões, incluindo padrões ambientais
PF 16.2 Considera taxa de variação			
Existem avaliações limitadas em andamento e separadas.	Em geral, os processos de negócios que mudam rapidamente são examinados com mais frequência do que aqueles que mudam lentamente.	Todos os grandes projetos de capital estão sujeitos a revisões na fase de planejamento.	Todos os principais projetos de TI estão sujeitos a revisão de acordo com a orientação do COBIT.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 16.3 Estabelece o entendimento básico			
Existem avaliações limitadas em andamento e separadas.	A administração tem uma compreensão geral do design e do estado atual do sistema de controle interno.	Existe documentação completa do projeto do sistema de controle interno que é atualizada para refletir as mudanças no desempenho do sistema.	A auditoria interna avalia e documenta a maturidade dos controles internos como parte de suas auditorias baseadas em sistemas.
PF 16.4 Usa pessoal experiente			
Existem avaliações limitadas em andamento e separadas.	A competência necessária para realizar avaliações contínuas e separadas é especificada nas descrições de cargo.	Todos os colaboradores recebem treinamento básico em avaliações contínuas de controle interno. Todo o pessoal de auditoria interna deve ter passado por um certo nível de competência para realizar o trabalho de auditoria.	A equipe selecionada recebe treinamento adicional sobre a melhor forma de realizar nossas avaliações separadas.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 16.5 Integra-se com o processo de negócios			
Existem avaliações limitadas em andamento e separadas.	Os gestores de primeira linha revisam os processos com base nos resultados de seu desempenho nas atividades de controle	A revisão dos riscos da segunda linha de defesa é realizada anualmente, a menos que as unidades de negócios estejam sujeitas a uma mudança rápida de liderança ou métodos de negócios.	Os planos estratégico e anual de auditoria interna ajustam o cronograma de revisões dos processos de negócios para refletir as revisões da administração.
PF 16.6 Ajusta escopo e frequência			
Existem avaliações limitadas em andamento e separadas.	A administração varia o escopo das avaliações separadas com base no tamanho e no tempo desde a última revisão.	O registro de riscos corporativos identifica os altos riscos para a organização e quando as políticas e processos relacionados foram revisados pela última vez.	Os planos estratégico e anual de auditoria interna são baseados na avaliação de riscos.
PF 16.7 Avalia objetivamente			
Existem avaliações limitadas em andamento e separadas.	A administração revisa os componentes do sistema de controle interno de forma cíclica.	A auditoria interna fornece uma avaliação anual da eficácia do sistema de controle interno e de cada componente do mesmo com base em seus exames durante o ano	Existe uma declaração anual de fiabilidade baseada na certificação da eficácia dos controlos internos por parte dos gestores individuais.

Princípio 17. A organização seleciona, avalia e comunica deficiências de controles internos em tempo hábil às partes responsáveis por tomar ações corretivas, incluindo a alta administração e as entidades reguladoras conforme apropriado

Nível 1: Informal *Ad-hoc/ Caótico*	**Nível 2: Definido** *Padrão/ Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 17.1 Avalia resultados			
Existem revisões limitadas dos resultados das avaliações contínuas e separadas.	Revisão da administração dos relatórios de auditoria interna dos resultados das auditorias baseadas em sistemas.	Revisão administrativa de relatórios pela segunda linha de defesa. Análise das causas de erros nas demonstrações financeiras identificadas pela SAI (auditoria externa).	Revisão da administração do relatório anual do comitê de auditoria sobre a eficácia do controle interno. Revisão periódica do cadastro de riscos corporativos.
PF 17.2 Comunica deficiências			
As deficiências não são comunicadas às entidades reguladoras.	Todos os relatórios de auditoria interna são enviados às unidades organizacionais auditadas para análise e recomendações de ações feitas.	São necessárias respostas formais da unidade organizacional auditada para todas as recomendações feitas.	A auditoria interna fornece às entidades reguladoras uma lista de todas as recomendações de auditoria pendentes (não implementadas) há mais de um ano.

Nível 1: Informal *Ad-hoc/Caótico*	**Nível 2: Definido** *Padrão/Repetível*	**Nível 3: Gerenciado e Monitorado** *Previsível*	**Nível 4: Otimizado** Eficiente/Eficaz
PF 17.3 Monitora ações corretivas			
Não há monitoramento de ações corretivas.	Existe um ponto focal na organização responsável por monitorar relatórios/recomendações de auditoria interna e segunda linha de defesa relacionados a controles internos.	A administração reporta às entidades reguladoras as razões pelas quais as recomendações da auditoria interna estão pendentes há mais de um ano.	A administração fornece uma declaração anual sobre a eficácia do controle interno às suas entidades reguladoras.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs,
Education and Research EAER
State Secretariat for Economic Affairs SECO

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

MINISTRY OF FINANCE
OF THE RUSSIAN FEDERATION

C