NORMA INTERNACIONAL DE AUDITORIA 315 (REVISTA 2019)

IDENTIFICAR E AVALIAR OS RISCOS DE DISTORÇÃO MATERIAL

(Eficaz para auditorias de demonstrações financeiras de períodos que iniciem em ou após 15 de dezembro de 2021)

ÍNDICE

Parágrafo

Introdução

Âmbito desta ISA 1

Principais conceitos desta ISA 2-8

Escalabilidade 9

Data de Eficácia 10

Objetivo 11

Definições 12

Requisitos

Procedimentos de Avaliação do Risco e Atividades Relacionadas 13-18

Obter um Entendimento da Entidade e do seu Ambiente, do Referencial de Relato Financeiro Aplicável e do seu Sistema de Controlo Interno 19-27

Identificar e Avaliar os Riscos de Distorção Material 28-37

Documentação 38

Material de Aplicação e Outro Material Explicativo

Definições A1-A10

Procedimentos de Avaliação do Risco e Atividades Relacionadas A11-A47

Obter um Entendimento da Entidade e do seu Ambiente, do Referencial de Relato Financeiro Aplicável e do seu Sistema de Controlo Interno A48-A183

Identificar e Avaliar os Riscos de Distorção Material A184-A236

Documentação A237-A241

Apêndice 1: Considerações para o Entendimento da Entidade e do seu Modelo de Negócio

Apêndice 2: Entendimento dos Fatores de Risco Inerente

Apêndice 3: Entendimento do Sistema de Controlo Interno da Entidade

Apêndice 4: Considerações para o Entendimento da Função de Auditoria Interna da Entidade

Apêndice 5: Considerações para o Entendimento das Tecnologias de Informação (TI)

Apêndice 6: Considerações para o Entendimento dos Controlos Gerais de TI

A Norma Internacional de Auditoria (ISA) 315 (Revista 2019), *Identificar e Avaliar os Riscos de Distorção Material*, deve ser lida no contexto da ISA 200, *Objetivos Gerais do Auditor Independente e Condução de uma Auditoria de Acordo com as Normas Internacionais de Auditoria*.

Introdução

Âmbito desta ISA

1. Esta Norma Internacional de Auditoria aborda a responsabilidade do auditor quanto à identificação e avaliação dos riscos de distorção material nas demonstrações financeiras.

Principais conceitos desta ISA

2. A ISA 200 trata dos objetivos gerais do auditor na realização de uma auditoria às demonstrações financeiras[1], incluindo a obtenção de provas de auditoria suficientes e apropriadas para reduzir o risco de auditoria para um nível aceitavelmente baixo[2]. O risco de auditoria é função dos riscos de distorção material e do risco de deteção[3]. A ISA 200 explica que os riscos de distorção material podem existir a dois níveis[4]: ao nível global das demonstrações financeiras; e ao nível de asserção para classes de transações, saldos de contas e divulgações.

3. A ISA 200 exige que o auditor exerça julgamento profissional ao planear e executar uma auditoria de demonstrações financeiras, e que planeie e execute uma auditoria com ceticismo profissional, reconhecendo que podem existir circunstâncias que originaram que as demonstrações financeiras estejam materialmente distorcidas[5].

4. Os riscos ao nível das demonstrações financeiras relacionam-se de forma generalizada com as demonstrações financeiras como um todo e afetam potencialmente várias asserções. Os riscos de distorção material ao nível das asserções consistem em dois componentes, risco inerente e risco de controlo:

   - O risco inerente é definido como a suscetibilidade de uma asserção relativa a uma classe de transações, saldo de conta ou divulgação a uma distorção que possa ser material, individualmente ou agregada com outras distorções, antes da consideração de quaisquer controlos relacionados.
   - O risco de controlo é definido como o risco de ocorrência de uma distorção relativa a uma classe de transações, saldo de conta ou divulgação e que possa ser material, individualmente ou agregada com outras distorções, não seja evitada ou detetada e corrigida em tempo oportuno pelo controlo interno da entidade.

5. A ISA 200 explica que os riscos de distorções materiais são avaliados ao nível da asserção, a fim de determinar a natureza, a oportunidade e a extensão de outros procedimentos de auditoria necessários para obter auditoria suficientes e apropriadas[6]. Para os riscos de distorção material identificados ao nível da asserção, esta norma existe uma avaliação separada do risco inerente e do risco de controlo. O grau de variação do risco inerente é referido nesta norma como a "escala de risco inerente".

6. Os riscos de erros materiais identificados e avaliados pelo auditor incluem quer os devidos a erros quer os devidos a fraude. Embora ambos sejam tratados por esta norma, a importância da fraude é tal que são incluídos requisitos e orientações adicionais na ISA 240[7] em relação aos procedimentos de avaliação de risco e atividades relacionadas para obter informações que são utilizadas para identificar, avaliar e responder aos riscos de distorção material devido a fraude.

7. O processo de identificação e avaliação do risco do auditor é iterativo e dinâmico. O entendimento do auditor sobre a entidade e o seu ambiente, sobre o referencial de relato financeiro aplicável e sobre o sistema de controlo interno da entidade são interdependentes com conceitos dentro dos requisitos para identificar e avaliar os riscos de distorção material. Ao obter o entendimento exigido por esta norma, podem ser desenvolvidas expectativas iniciais de riscos, as quais podem ser ajustadas à medida que o auditor avança no processo de identificação e avaliação de riscos. Adicionalmente, esta norma e a ISA 330 exigem que o auditor reveja a avaliação do risco, e adapte as suas respostas globais e procedimentos adicionais de auditoria, com base em provas de auditoria obtidas através da realização de mais procedimentos de auditoria em conformidade com a ISA 330, ou se forem obtidas novas informações.

8. A ISA 330 exige que o auditor conceba e implemente respostas globais para tratar os riscos de distorção material avaliados ao nível das demonstrações financeiras [8]. A ISA 330 explica ainda que a avaliação dos riscos de

---

1 ISA 200, Objetivos Gerais do Auditor Independente e Condução de uma Auditoria de Acordo com as Normas Internacionais de Auditoria
2 ISA 200, parágrafo 17
3 ISA 200, parágrafo 13 (m)
4 ISA 200, parágrafo A37
5 ISA 200, parágrafo 15 e 16
6 ISA 200, parágrafo A46 e ISA 330, *As Respostas do Auditor a Riscos Avaliados*, parágrafo 6
7 ISA 240, *As Responsabilidades do Auditor Relativas a Fraude numa Auditoria de Demonstrações Financeiras*
8 ISA 330, parágrafo 5

distorção material ao nível das demonstrações financeiras, e as respostas globais do auditor, é afetada pelo conhecimento que o auditor tem do ambiente de controlo. A ISA 330 também exige que o auditor conceba e execute procedimentos de auditoria adicionais cuja natureza, oportunidade e extensão se baseiam e respondem aos riscos de distorção material avaliados ao nível de asserção[9].

Escalabilidade

9. A ISA 200 afirma que algumas ISA incluem considerações sobre a escalabilidade que ilustram a aplicação dos requisitos a todas as entidades, independentemente da sua natureza e de as circunstâncias serem menos complexas ou mais complexas[10]. Esta norma aplica-se a auditorias de todas as entidades, independentemente da sua dimensão ou complexidade, pelo que o material de aplicação incorpora considerações específicas tanto para entidades menos complexas como para entidades mais complexas, sempre que apropriado. Embora a dimensão de uma entidade possa ser um indicador da sua complexidade, algumas entidades mais pequenas podem ser complexas e algumas entidades maiores podem ser menos complexas

Data de Eficácia

10. Esta ISA é eficaz para auditorias de demonstrações financeiras de períodos que iniciem em ou após 15 de dezembro de 2021.

Objetivo

11. O objetivo do auditor é identificar e avaliar os riscos de distorção material devido a fraude ou a erro, ao nível das demonstrações financeiras e ao nível de asserção, proporcionando assim uma base para conceber e implementar respostas aos riscos de distorção material avaliados.

Definições

12. Para efeito das ISA, são aplicáveis as seguintes definições:

(a) *Asserções* – Declarações, de forma explícita ou outra, relativas ao reconhecimento, mensuração, apresentação e divulgação de informações que são incorporadas nas demonstrações financeiras que são inerentes à declaração pelo órgão de gestão de que as demonstrações financeiras estão apresentadas de acordo com o referencial de relato financeiro aplicável. As asserções são usadas pelo auditor para considerar os diferentes tipos de distorções materiais que podem ocorrer quando identificam, avaliam e respondem aos riscos de distorção material. (Ref: Parágrafo A1)

(b) *Risco de negócio* - Risco resultante de condições, acontecimentos, circunstâncias, ações ou inações significativas que possam afetar adversamente a capacidade de uma entidade para atingir os seus objetivos e executar as suas estratégias, ou para fixar objetivos e estratégias não apropriados.

(c) *Controlos* – Políticas ou procedimentos que uma entidade implementa para atingir os objetivos de controlo do órgão de gestão ou dos encarregados da governação. Neste contexto: (Ref: Parágrafos A2-A5)

(i) Políticas são afirmações sobre o que deve, ou não deve, ser feito dentro da entidade para efetuar o controlo. Essas afirmações podem estar documentadas, explicitamente incluídas em comunicações, ou implícitas nas ações e decisões.

(ii) Procedimentos são ações para implementar as políticas.

(d) *Controlos gerais das tecnologias de informação (TI)* - Controlos sobre os processos de TI da entidade que suportam o funcionamento contínuo adequado do ambiente de TI, incluindo o funcionamento contínuo e eficaz dos controlos sobre o processamento de informação e a integridade da informação (ou seja, a plenitude, a exatidão e validade da informação) no sistema de informação da entidade. Ver também a definição de ambiente TI.

(e) *Controlos sobre o processamento de informação* - Controlos relativos ao processamento de informação em aplicações TI ou em processos de informação manuais nos sistemas de informação da entidade que abordam diretamente os riscos para a integridade da informação (ou seja, a plenitude, a exatidão e validade das transações e outras informações). (Ref: Parágrafo A6)

(f) *Fatores de risco inerente* – Características de eventos ou condições que afetam a suscetibilidade da distorção, quer seja devido a fraude ou a erro, de uma asserção sobre uma classe de transações, saldo de

[9] ISA 330, parágrafo 6
[10] ISA 200, parágrafo A69

conta ou divulgação, antes de se considerar os controlos. Tais fatores podem ser qualitativos ou quantitativos, e incluem complexidade, subjetividade, alteração, incerteza ou suscetibilidade a distorções, devido a enviesamentos de gestão ou outros fatores de risco de fraude[11], na medida em que afetem o risco inerente. (Ref: Parágrafos A7–A8)

(g) *Ambiente de TI* - As aplicações TI e a infraestrutura TI de suporte, bem como os processos TI e o pessoal envolvido nesses processos, que uma entidade utiliza para suportar as operações comerciais e atingir as estratégias comerciais. Para os fins desta norma:

(i) Uma aplicação TI é um programa ou um conjunto de programas que são usados na iniciação, processamento, registo e reporte de transações ou informação. Aplicações TI incluem armazenamento de dados e geradores de relatórios.

(ii) A infraestrutura de TI inclui a rede, os sistemas operativos, as bases de dados e os respetivos hardware e software.

(iii) Os processos TI são os processos de uma entidade para gerir o acesso ao ambiente TI, gerir as alterações aos programas ou alterações ao ambiente TI e gerir as operações TI.

(h) *Asserções relevantes* – Uma asserção sobre uma classe de transações, saldo de conta ou divulgação é relevante quando tem identificado um risco de distorção material. A determinação se uma asserção é relevante é efetuada antes de considerar quaisquer controlos relacionados (ou seja, o risco inerente). (Ref: Parágrafo A9)

(i) *Riscos decorrentes da utilização de TI* - Suscetibilidade de os controlos sobre o processamento de informação para a conceção ou operação ineficazes, ou os riscos associados à integridade da informação (ou seja, a plenitude, a exatidão e validade das transações e outras informações) no sistema de informação da entidade, devido a uma conceção ou operação ineficaz dos controlos nos processos de TI da entidade (ver ambiente de TI).

(j) *Procedimentos de avaliação do risco* – Os procedimentos de auditoria concebidos e executados para identificar e avaliar os riscos de distorção material, seja devido a fraude ou erro, quer a nível das demonstrações financeiras quer a nível de asserção.

(k) *Classes de transações, contas e divulgações significativas* – Uma classe de transações, saldo de conta ou divulgação para a qual existe uma ou mais asserções relevantes.

(l) *Risco significativo* – Um risco de distorção material identificado: (Ref: Parágrafo A10)

(i) Para o qual a avaliação do risco inerente está próxima do limite superior da escala de risco inerente, devido ao grau em que os fatores de risco inerentes afetam a combinação da probabilidade de ocorrência da distorção e da magnitude da potencial distorção, caso essa distorção ocorra; ou

(ii) Que deva ser tratado como risco significativo de acordo com outras ISA.[12]

(m) *Sistema de controlo interno* – O sistema concebido, implementado e mantido pelos encarregados da governação, órgão de gestão e outro pessoal, para proporcionar segurança razoável acerca da consecução dos objetivos de uma entidade com respeito à fiabilidade do reporte financeiro, eficácia e eficiência das operações e cumprimento das leis e regulamentos aplicáveis. Para os efeitos das ISA, o sistema de controlo interno é composto por cinco componentes inter-relacionados:

(i) Ambiente de controlo;

(ii) O processo da entidade para avaliação do risco;

(iii) O processo da entidade para monitorização do sistema de controlo interno;

(iv) O sistema de informação e de comunicação; e

(v) As atividades de controlo.

[11] ISA 240, parágrafos A24–A27

[12] ISA 240, parágrafo 27 e ISA 550, *Partes Relacionadas*, parágrafo 18

Requisitos

Procedimentos de Avaliação do Risco e Atividades Relacionadas

13. O auditor deve conceber e executar procedimentos de avaliação do risco para obter prova de auditoria que proporcione uma base para: (Ref: Parágrafos A11-A18)

    (a) A identificação e avaliação dos riscos de distorção material, seja devido a fraude ou erro, ao nível das demonstrações financeiras e ao nível da asserção; e

    (b) O desenho de procedimentos adicionais de acordo com a ISA 330.

    O auditor deve conceber e executar procedimentos de avaliação de risco de uma forma que não enviesada para a obtenção de provas de auditoria que possam ser corroborativas ou para a exclusão de provas de auditoria que possam ser contraditórias (Ref: Parágrafo A14)

14. Os procedimentos de avaliação do risco devem incluir: (Ref: Parágrafos A19–A21)

    (a) Indagações ao órgão de gestão e a outros indivíduos apropriados dentro da entidade, incluindo indivíduos dentro da função de auditoria interna (se esta função existir). (Ref: Parágrafos A22-A26)

    (b) Procedimentos analíticos; e (Ref: Parágrafos A2-A31)

    (c) Observação e inspeção. (Ref: Parágrafos A32-A36)

Informações de outras fontes

15. Quando obtém prova de auditoria de acordo com o parágrafo 13, o auditor deve considerar a informação obtida: (Ref: Parágrafos A37-A38)

    (a) Nos procedimentos do auditor relativos à aceitação ou continuação do relacionamento com o cliente ou do trabalho de auditoria; e.

    (b) Quando aplicável, em outros trabalhos executados pelo sócio responsável para a entidade.

16. Quando o auditor pretender usar informação obtida da sua experiência anterior com a entidade e dos procedimentos de auditoria executados em auditorias anteriores, o auditor deve avaliar se essa informação ainda é relevante e fiável como prova de auditoria para a auditoria corrente. (Ref: Parágrafos A39–A41)

Discussões da equipa de auditoria

17. O sócio responsável pelo trabalho e outros membros chave da equipa de trabalho devem discutir a aplicação do referencial de relato financeiro aplicável e a suscetibilidade das demonstrações financeiras da entidade a distorção material. (Ref: Parágrafos A42-A47)

18. Quando existem membros da equipa de trabalho não envolvidos na discussão, o sócio responsável pelo trabalho deve determinar quais as matérias que devem ser comunicadas àqueles membros.

Obtenção de Conhecimento Sobre da Entidade e do Seu Ambiente, o Referencial de Relato Financeiro Aplicável e o Sistema de Controlo Interno da Entidade (Ref: Parágrafos A4-A49)

Entendimento da Entidade e do Seu Ambiente, e do Referencial de Relato Financeiro Aplicável (Ref: Parágrafos A50-A55)

19. O auditor deve executar procedimentos de avaliação do risco para obter um entendimento sobre:

    (a) Os seguintes aspetos sobre a entidade e o seu ambiente:

        (i) A estrutura organizacional da entidade, propriedade e estrutura de governação, e o seu modelo de negócio, incluindo a extensão em que o modelo de negócio integra o uso de TI; (Ref: Parágrafos A56-A67)

        (ii) Indústria, regulação e outros fatores externos; (Ref: Parágrafos A68-A73) e

        (iii) Os indicadores usados, internos e externos, para avaliar a performance financeira da entidade; (Ref: Parágrafos A74-A81)

    (b) O referencial de relato financeiro aplicável, e as políticas contabilísticas da entidade e as razões para alterações às mesmas; (Ref: Parágrafos A82-A84) e

(c) Como o risco inerente afetam a suscetibilidade de distorções nas asserções e o grau em que são afetadas na preparação das demonstrações financeiras, de acordo com o referencial de relato financeiro aplicável, baseado no entendimento obtido em (a) e (b). (Ref: Parágrafos A85-A89)

20. O auditor deve avaliar se as políticas contabilísticas da entidade são apropriadas e consistentes com o referencial de relato financeiro aplicável.

Entender os Componentes do Sistema de Controlo Interno da Entidade (Ref: Parágrafos A90-A95)

Ambiente de Controlo, o Processo da Entidade para Avaliação do Risco e o Processo da Entidade para Monitorização do Sistema de Controlo Interno (Ref: Parágrafos A96-A98)

Ambiente de Controlo

21. O auditor deve obter um entendimento do ambiente de controlo relevante para a elaboração das demonstrações financeiras, através da realização de procedimentos de avaliação de risco	
(a) Compreendendo o conjunto de controlos, processos e estruturas que abordam: (Ref: Parágrafos A101–A102) (i) Como são exercidas as responsabilidades de supervisão da gestão, tais como a cultura da entidade e o compromisso da gestão com a integridade e os valores éticos; (ii) Quando os responsáveis pela governação estão separados da gestão, a independência e a supervisão do sistema de controlo interno da entidade por parte dos responsáveis pela governação; (iii) A atribuição de autoridade e responsabilidade pela entidade; (iv) Como a entidade atrai, desenvolve e retém indivíduos competentes; e (v) Como é que a entidade responsabiliza os indivíduos pelas suas responsabilidades na prossecução dos objetivos do sistema de controlo interno;	e (b) Avaliando: (Ref: Parágrafos A103–A108) (i) Se a gestão, com a supervisão dos responsáveis pela governação, criou e manteve uma cultura de honestidade e comportamento ético; (ii) Se o ambiente de controlo fornece uma base apropriada para os outros componentes do sistema de controlo interno da entidade, considerando a natureza e complexidade da entidade; e (iii) Se as deficiências de controlo identificadas no ambiente de controlo afetam os outros componentes do sistema de controlo interno da entidade.

O processo da entidade para avaliação do risco

22. O auditor deve obter um entendimento do processo da entidade para avaliação do risco relevante para a elaboração das demonstrações financeiras, através da realização de procedimentos de avaliação de risco:	
(a) Compreendendo os processos da entidade: (Ref: Parágrafos A109–A110) (i) Para a identificação dos riscos de negócio relevantes para os objetivos de informação financeira (Ref: Parágrafo A62) (ii) Para avaliar a relevância desses riscos, incluindo a probabilidade da sua ocorrência; e (iii) Para abordar esses riscos;	e (b) Avaliando se o processo da entidade para avaliação do risco é adequado às circunstâncias da entidade, tendo em conta a natureza e complexidade da entidade. (Ref: Parágrafos A111–A113)

23. Se o auditor identificar riscos de distorção material que o órgão de gestão não identificou, o auditor deve:

(a) Determinar se esses riscos são de natureza tal que seria de esperar que fossem identificados pelo processo da entidade para avaliação do risco e, se sim, obter um entendimento da razão porque o processo da entidade para avaliação do risco falhou na identificação desse risco de distorção material; e

(b) Ter em consideração as implicações da avaliação do parágrafo 22(b).

O Processo da Entidade para Monitorização do Sistema de Controlo Interno

24. O auditor deve obter um entendimento do processo da entidade para monitorização do sistema de controlo interno relevante para a elaboração das demonstrações financeiras, através da realização de procedimentos de avaliação de risco: (Ref: Parágrafos A114–A115)	
(a) Compreendendo os aspetos do processo da entidade que abordam: (i) Avaliações contínuas e separadas para monitorizar a eficácia dos controlos, e a identificação e remediação das deficiências de controlo identificadas; (Ref: Parágrafos A116–A117) (ii) A função de auditoria interna da entidade, se existir, incluindo a sua natureza, responsabilidades e atividades; (Ref: Parágrafo A118) (b) Compreendendo as fontes de informação utilizadas no processo da entidade para monitorização do sistema de controlo interno, e a base sobre a qual a gestão considera que a informação é suficientemente fiável para o efeito; (Ref: Parágrafos A119–A120)	e (c) Avaliando se o processo da entidade para monitorização do sistema de controlo interno é adequado às circunstâncias da entidade, tendo em conta a natureza e complexidade da entidade. (Ref: Parágrafos A121–A122)

O sistema de informação e de comunicação e as atividades de controlo (Ref: Parágrafos A123–A130)

O sistema de informação e de comunicação

25. O auditor deve obter uma compreensão do sistema de informação e comunicação da entidade relevante para a elaboração das demonstrações financeiras, através da realização de procedimentos de avaliação de risco: (Ref: Parágrafo A131)	
(a) Compreendendo as atividades de processamento de informação da entidade, incluindo os seus dados e informações, os recursos a utilizar em tais atividades e as políticas que definem, para classes de transações significativas, saldos de contas e divulgações: (Ref: Parágrafos A132-A143) (i) Como a informação flui através do sistema de informação da entidade, incluindo como: a. As transações são iniciadas, e como a informação sobre elas é registada, processada, corrigida conforme necessário, incorporada no balancete do razão geral e reportada nas demonstrações financeiras; e	e (c) Avaliando se o sistema de informação e comunicação da entidade suporta adequadamente a preparação das demonstrações financeiras da entidade, de acordo com o referencial de relato financeiro aplicável. (Ref: Parágrafo A146)

b. As informações sobre eventos e condições, para além das transações, são capturadas, processadas e divulgadas nas demonstrações financeiras; (ii) Os registos contabilísticos, contas específicas nas demonstrações financeiras e outros registos de suporte relacionados com os fluxos de informação no sistema de informação; (iii) O processo de reporte financeiro utilizado para preparar as demonstrações financeiras da entidade, incluindo as divulgações; e (iv) Os recursos da entidade, incluindo o ambiente TI, relevantes para (a)(i) a (a)(iii) acima; (b) Compreendendo como a entidade comunica os assuntos significativos que apoiam a preparação das demonstrações financeiras e as responsabilidades relacionadas com o reporte no sistema de informação e outros componentes do sistema de controlo interno: (Ref: Parágrafos A144-A145) (i) Entre pessoas dentro da entidade, incluindo a forma como as funções e responsabilidades de relato financeiro são comunicadas; (ii) Entre a gestão e os responsáveis pela governação; e (iii) Com entidades externas, tais como as que têm entidades reguladoras;	

As atividades de controlo

26. O auditor deve obter a compreensão da componente de atividades de controlo, através da realização de procedimentos de avaliação de risco: (Ref: Parágrafos A147-A157)	
(a) Identificando os controlos que abordam os riscos de distorções materiais ao nível da asserção na componente de atividades de controlo, como se segue: (i) Controlos que abordam um risco avaliado como sendo um risco significativo; (Ref: Parágrafos A158-A159) (ii) Controlos sobre lançamentos de diário, incluindo lançamentos de diário não usuais utilizados para registar transações ou ajustamentos não recorrentes e não	e (d) Para cada controlo identificado em (a) ou (b): (Ref: Parágrafos A175-A181) (i) Avaliar se o controlo foi concebido eficazmente para fazer face ao risco de distorção material ao nível da asserção, ou se foi concebido eficazmente para apoiar o funcionamento de outros controlos; e (ii) Determinar se o controlo foi implementado, através da realização de procedimentos para

usuais; (Ref: Parágrafos A160-A161) (iii) Controlos para os quais o auditor planeia testar a eficácia operacional na determinação da natureza, tempestividade e extensão dos testes substantivos, os quais devem incluir controlos que abordem os riscos para os quais os procedimentos substantivos, por si só, não forneçam provas de auditoria suficientes e adequadas; e (Ref: Parágrafos A162-A164) (iv) Outros controlos que o auditor considere adequados para permitir ao auditor cumprir os objetivos do parágrafo 13 relativamente aos riscos ao nível da asserção, com base no julgamento profissional do auditor; (Ref: Parágrafo A165) (b) Com base nos controlos identificados em (a), identificando as aplicações informáticas e os outros aspetos do ambiente TI da entidade que estão sujeitos a riscos decorrentes da utilização de TI; (Ref: Parágrafos A166-A172) (c) Para tais aplicações TI e outros aspetos do ambiente TI identificados em (b), identificar: (Ref: Parágrafos A173-A174) (i) Os riscos relacionados decorrentes da utilização de TI; e (ii) Os controlos TI gerais da entidade que abordam tais riscos;	além da inquisição ao pessoal da entidade.

Deficiências de Controlo no Sistema de Controlo Interno da Entidade

27. Com base na avaliação do auditor a cada um dos componentes do sistema de controlo interno da entidade, o auditor deve determinar se foram identificadas uma ou mais deficiências de controlo. (Ref: Parágrafos A182-A183)

Identificar e Avaliar os Riscos de Distorção Material (Ref: Parágrafos A184-A185)

Identificar os Riscos de Distorção Material

28. O auditor deve identificar os riscos de distorção material e avaliar se eles existem: (Ref: Parágrafos A186-A192)
    (a) Ao nível das demonstrações financeiras; (Ref: Parágrafos A193-A200) ou
    (b) Ao nível da asserção para as classes de transações, saldos de contas e divulgações. (Ref: Parágrafo A201)
29. O auditor deve determinar as asserções relevantes e as classes de transações, saldos de contas e divulgações significativas relacionadas. (Ref: Parágrafos A202-A204)

Avaliar os riscos de distorção materiais ao nível das demonstrações financeiras

30. Para os riscos identificados de distorção material ao nível das demonstrações financeiras, o auditor deve avaliar o risco e: (Ref: Parágrafos A193-A200)
    (a) Determinar se esses riscos afetam a avaliação do risco ao nível das asserções; e
    (b) Avaliar a natureza e extensão do seu efeito generalizado sobre as demonstrações financeiras.

Avaliar os riscos de distorção materiais ao nível das asserções

Avaliação do Risco Inerente (Ref: Parágrafos A205-A217)

31. Para os riscos identificados de distorção material ao nível das asserções, o auditor deve avaliar o risco inerente avaliando a probabilidade e a magnitude da distorção. Ao fazê-lo, o auditor deve ter em consideração como, e em que medida:

    (a) Os fatores de risco inerente afetam a suscetibilidade das asserções à distorção; e

    (b) O risco de distorção material ao nível das demonstrações financeiras afeta a avaliação do risco inerente aos riscos de distorção materiais ao nível das asserções. (Ref: Parágrafos A215-A216)

32. O auditor deve determinar se algum dos riscos avaliados de distorção material constitui um risco significativo. (Ref: Parágrafos A218-A221)

33. O auditor deve determinar se os procedimentos substantivos por si não podem fornecer prova de auditoria adequada e suficiente para qualquer dos riscos de distorção material ao nível das asserções. (Ref: Parágrafos A222-A225)

Avaliação do risco de controlo

34. Se o auditor planeia testar a eficácia operacional dos controlos, o auditor deve avaliar o risco de controlo. Se o auditor não planear testar a eficácia operacional dos controlos, a avaliação do risco de controlo pelo auditor deve ser tal que a avaliação do risco de distorção material seja a mesma que a avaliação do risco inerente. (Ref: Parágrafos A226-A229)

Avaliar a Prova de Auditoria Obtida nos Procedimentos de Avaliação do Risco

35. O auditor deve avaliar de a prova de auditoria obtida nos procedimentos de avaliação do risco proporciona as bases para a identificação e avaliação do risco de distorção material. Se não proporciona, o auditor deve executar procedimentos de avaliação do risco adicionais até que prova de auditoria tenha sido obtida que proporcione tal base. Na identificação e avaliação do risco de distorção material, o auditor deve ter em conta toda a prova de auditoria obtida dos procedimentos de avaliação do risco, quer corroborativas quer contraditórias com afirmações feitas pela gestão. (Ref: Parágrafos A230-A232)

Classes de Transações, Saldos de contas e Divulgações que Não Sejam Significativas mas que Sejam Materiais

36. Para classes de transações, saldos de contas ou divulgações materiais que não tenham sido avaliadas como sendo classes de transações, saldos de contas ou divulgações significativas, o auditor deverá avaliar se a avaliação do auditor continua a ser apropriada. (Ref: Parágrafos A233-A235)

Revisão da Avaliação do Risco

37. Se o auditor obtém novas informações que sejam inconsistentes com a prova de auditoria que serviu de base ao auditor na identificação ou avaliação do risco de distorção material, o auditor deve rever a identificação ou avaliação. (Ref: Parágrafo A236)

Documentação

38. O auditor deve incluir na documentação de auditoria:[13] (Ref: Parágrafos A237-A241)

    (a) A discussão entre a equipa de trabalho, e as decisões relevantes tomadas;

    (b) Os principais elementos do conhecimento do auditor de acordo com os parágrafos 19, 21, 22, 24 e 25; as fontes de informação a partir das quais o auditor obteve o seu conhecimento e os procedimentos de avaliação do risco executados;

    (c) A avaliação do desenho dos controlos identificados, e a determinação se tais controlos foram implementados, de acordo com o parágrafo 26; e

    (d) Os riscos de distorção material identificados e avaliados ao nível das demonstrações financeiras e ao nível de asserção, incluindo os riscos significativos e riscos para os quais os procedimentos substantivos de auditoria, por si só, não proporcionam prova de auditoria adequada e suficiente, e o racional para os julgamentos significativos efetuados.

***

[13] ISA 230, Documentação de Auditoria, parágrafos 8 -11, e A6-A7

Material de Aplicação e Outro Material Explicativo

Definições (Ref: Parágrafo 12)

Asserções (Ref: Parágrafo 12 (a))

A1. Categorias de asserções são usadas pelos auditores para considerar diferentes tipos de distorções potenciais que podem ocorrer na identificação, avaliação e resposta aos riscos de distorção material. Exemplos destas categorias de asserções estão descritos no parágrafo A190. As asserções são diferentes das declarações escritas requeridas pela ISA 580[14] para confirmar certos assuntos ou para suportar outra prova de auditoria.

Controlos (Ref: Parágrafo 12 (c))

A2. Os controlos estão incorporados nos componentes do sistema de controlo interno da entidade.

A3. As políticas são implementadas através das ações do pessoal dentro da entidade, ou através de restrições ao pessoal a tomar medidas que entrariam em conflito com tais políticas.

A4. Os procedimentos podem ser impostos, através de documentação formal ou de outra comunicação por parte da gestão ou dos responsáveis pela governação, ou podem resultar de comportamentos que não são impostos mas que são condicionados pela cultura da entidade. Os procedimentos podem ser aplicados através das ações permitidas pelas aplicações TI utilizadas pela entidade ou outros aspetos do ambiente TI da entidade.

A5. Os controlos podem ser diretos ou indiretos. Os controlos diretos são controlos que são suficientemente precisos para endereçar os riscos de distorções materiais ao nível das asserções. Os controlos indiretos são controlos que apoiam os controlos diretos.

Controlos de Processamento da Informação (Ref: Parágrafo 12 (e))

A6. Os riscos para a integridade da informação decorrem da suscetibilidade a uma implementação ineficaz das políticas de informação da entidade, que são políticas que definem os fluxos de informação, registos e processos de reporte no sistema de informação da entidade. Os controlos de processamento de informação são procedimentos que apoiam a implementação eficaz das políticas de informação da entidade. Os controlos de processamento da informação podem ser automáticos (ou seja, incorporados em aplicações TI) ou manuais (por exemplo, controlos de input ou output) e podem depender de outros controlos, incluindo outros controlos de processamento da informação ou controlos TI gerais.

Fatores de Risco Inerente (Ref: Parágrafo 12 (f))

O Apêndice 2 estabelece outras considerações relacionadas com o entendimento dos fatores de risco inerente.

A7. Os fatores de risco inerente podem ser qualitativos ou quantitativos e afetar a suscetibilidade das asserções a distorções. Fatores de risco inerente qualitativos relacionados com a preparação de informação requerida pelo referencial contabilístico aplicável incluem:

- Complexidade;
- Subjetividade;
- Alteração;
- Incerteza; ou
- Suscetibilidade a distorções devido à imparcialidade de gestão ou outros fatores de risco de fraude, na medida em que afetem o risco inerente.

A8. Outros fatores de risco de fraude, que afetem a suscetibilidade de distorções de uma asserção sobre uma classe de transações, saldo de conta ou divulgação podem incluir:

- A significância quantitativa ou qualitativa da classe de transações, saldo de conta ou divulgação; ou
- O volume ou a falta de uniformidade na composição dos itens que são processados pela classe de transações ou saldo de conta ou para serem refletidos na divulgação.

Asserções Relevantes (Ref: Parágrafo 12 (h))

A9. Um risco de distorção material pode estar relacionado com mais de uma asserção, situação em que todas as

[14] ISA 580, Declarações escritas

asserções com as quais esse risco se relaciona são asserções relevantes. Se uma asserção não tem identificado qualquer risco de distorção material, então não é uma asserção relevante.

Risco Significativo (Ref: Parágrafo 12 (l))

A10. Significância pode ser descrita como a importância relativa de um assunto, e é julgada pelo auditor no contexto em que esse assunto está a ser considerado. Para o risco inerente, a significância pode ser considerada no contexto de como, e em que medida, os fatores de risco inerente afetam a combinação da probabilidade de ocorrência de uma distorção e a magnitude da potencial distorção caso essa distorção ocorra.

Procedimentos de Avaliação do Risco e Atividades Relacionadas (Ref: Parágrafos 13-18)

A11. Os riscos de distorção material a serem identificados e avaliados incluem os riscos devidos fraude e os riscos devidos a erro, ambos cobertos por esta ISA. Porém, a importância da questão da fraude é tal que a ISA 240 inclui requisitos e orientações adicionais relativos a procedimentos de avaliação do risco e atividades relacionadas para obter informação que é usada para identificar e avaliar os riscos de distorção material devido a fraude.[15] Adicionalmente, as seguintes ISA fornecem requisitos e orientações adicionais para a identificação e avaliação do risco de distorção material no que respeita a questões e circunstâncias específicos:

- ISA 540 (Revista)[16] no que respeita a estimativas contabilísticas;
- ISA 550 no que respeita a relacionamentos e transações com partes relacionadas;
- ISA 570 (Revista)[17] no que respeita à continuidade; e
- ISA 600 (Revista)[18] no que respeita a demonstrações financeiras de grupos.

A12. O ceticismo profissional é necessário para uma avaliação crítica das provas de auditoria recolhidas na execução dos procedimentos de avaliação do risco, e auxilia o auditor a manter-se em alerta a provas de auditoria que não estejam enviesadas para corroborar a existência de riscos ou que possam ser contraditórias à existência de riscos. O ceticismo profissional é uma atitude aplicada pelo auditor quando aplica julgamentos profissionais que proporcionam a base para as ações do auditor. O auditor aplica o julgamento profissional ao determinar quando o auditor tem provas de auditoria que proporcionam uma base apropriada para a avaliação de riscos.

A13. A aplicação do ceticismo profissional pelo auditor inclui:

- Questionar informação contraditória e a fiabilidade de documentos;
- Considerar as respostas às indagações e outra informação obtida da gestão e dos encarregados pela governação;
- Estar atento a condições que possam indicar a possibilidade de distorções devidas a fraude ou erro; e
- Considerar se a prova de auditoria obtida suporta a sua identificação e avaliação do risco de distorção material, no contexto da natureza da entidade e das circunstâncias.

Porque é importante obter prova de auditoria de forma não enviesada (Ref: Parágrafo 13)

A14. Conceber e executar procedimentos de avaliação do risco para obter prova de auditoria que suporte a identificação e a avaliação do risco de distorção material de forma não enviesada pode auxiliar o auditor na identificação de informação potencialmente contraditória, que pode auxiliar o auditor a exercer o seu ceticismo profissional na identificação e avaliação do risco de distorção material.

Fontes de prova de auditoria (Ref: Parágrafo 13)

A15. Conceber e executar procedimentos de avaliação do risco para obter prova de auditoria de forma não enviesada pode passar por obter prova de múltiplas fontes internas e externas à entidade. Contudo, ao auditor não é exigido que efetue uma procura exaustiva para identificar todas as possíveis fontes de prova de auditoria. Adicionalmente à informação obtida de outras fontes[19], as fontes de informação para os procedimentos de avaliação do risco podem incluir:

- Interações com a gestão, com os encarregados pela governação, e outro pessoal-chave da entidade, tais

---

15 ISA 240, parágrafos 12-27

16 ISA 540 (Revista)*, Auditar Estimativas Contabilísticas e Respetivas Divulgações*

17 ISA 570 (Revista), *Continuidade*

18 ISA 600 (Revista), *Considerações Especiais – Auditorias de Demonstrações Financeiras de Grupos (Incluindo o Trabalho de Auditores de Componentes)*

19 Ver parágrafos A37 e A38.

como os auditores internos;

- Certas partes externas como reguladores, quer obtida direta ou indiretamente;
- Informação pública disponível sobre a entidade, por exemplo comunicados de imprensa emitidos pela entidade, materiais para analistas ou reuniões com grupos de investidores, relatórios de analistas ou informações sobre a atividade comercial;

Independentemente da fonte de informação, o auditor deve considerar a relevância e a fiabilidade da informação a usar como prova de auditoria de acordo com a ISA 500.[20]

Escalabilidade (Ref: Parágrafo 13)

A16. A natureza e extensão dos procedimentos de avaliação de risco varia com base na natureza e circunstâncias da entidade (por exemplo, a formalidade das políticas e procedimentos da entidade e processos e sistemas). O auditor aplica o julgamento profissional para determinar a natureza e a extensão dos procedimentos de avaliação de risco a serem executados para cumprir os requisitos desta ISA.

A17. Embora a extensão da formalização das políticas e procedimentos e dos processos e sistemas de uma entidade possa variar, ao auditor é ainda exigida a obtenção de um entendimento de acordo com os parágrafos 19, 21, 22, 24, 25 e 26.

> **Exemplos**:
>
> Algumas entidades, incluindo entidades menos complexas, e particularmente entidades geridas pelo proprietário, podem não ter estabelecido processos e sistemas estruturados (por exemplo, um processo de avaliação de risco ou um processo para monitorizar o sistema de controlo interno) ou podem ter estabelecido processos ou sistemas com documentação limitada ou pode existir uma falta de coerência na forma como são realizados. Quando tais sistemas e processos carecem de formalidade, o auditor pode ainda assim ser capaz de efetuar procedimentos de avaliação de risco através de observação e indagação.
>
> Outras entidades, normalmente entidades mais complexas, deverão ter políticas e procedimentos mais formalizados e documentados. O auditor pode utilizar essa documentação na realização de procedimentos de avaliação de risco.

A18. A natureza e extensão dos procedimentos de avaliação de risco a serem realizados no primeiro ano de um trabalho pode ser mais extensa do que os procedimentos para um trabalho recorrente. Em períodos subsequentes, o auditor pode concentrar-se em alterações que tenham ocorrido desde o período anterior

Tipos de Procedimentos de Avaliação do Risco (Ref: Parágrafo 14)

A19. ISA 500[21] explica os tipos de procedimentos de auditoria que podem ser realizados na obtenção de provas de auditoria a partir de procedimentos de avaliação de risco e outros procedimentos de auditoria. A natureza, a tempestividade e a extensão dos procedimentos de auditoria podem ser afetados pelo facto de alguns dos dados contabilísticos e outras provas poderem estar disponíveis apenas em formato eletrónico ou apenas em determinados momentos[22]. O auditor pode efetuar procedimentos substantivos ou testes de controlo, em conformidade com a ISA 330, em simultâneo com procedimentos de avaliação de risco, quando for eficiente fazê-lo. As provas de auditoria obtidas que suportam a identificação e avaliação dos riscos de declarações incorretas materiais podem igualmente apoiar a deteção de distorções materiais ao nível da asserção ou a avaliação da eficácia operacional dos controlos.

A20. Embora se exija ao auditor que execute todos os procedimentos de avaliação do risco descritos no parágrafo 14 no decurso da obtenção do entendimento da entidade e do seu ambiente, sobre o referencial de relato financeiro aplicável e sobre o sistema de controlo interno da entidade (ver os parágrafos 19 a 26), não se exige que o auditor execute todos esses procedimentos relativamente a cada aspeto desse conhecimento. Podem ser executados outros procedimentos quando a informação a ser obtida possa ser útil na identificação de riscos de distorção material. Exemplos de tais procedimentos podem incluir fazer indagações junto do consultor jurídico externo ou supervisores externos da entidade, ou de peritos avaliadores que a entidade tenha usado.

Ferramentas e Técnicas Automatizadas (Ref: Parágrafo 14)

A21. Utilizando ferramentas e técnicas automatizadas, o auditor pode efetuar procedimentos de avaliação de risco

[20] ISA 500, *Prova de Auditoria*, parágrafo 7
[21] ISA 500, parágrafos A14–A17 e A21–A25
[22] ISA 500, parágrafo A16

sobre grandes volumes de informação (do diário do razão geral, de diários auxiliares ou de outra informação operacional) incluindo para análise, recálculos, reexecução ou reconciliação.

Indagações ao Órgão de Gestão e a Outras Pessoas da Entidade (Ref: Parágrafo 14 (a))

Porque São Efetuadas Indagações Sobre a Gestão e Outras Pessoas Dentro da Entidade

A22. A informação obtida pelo auditor para suportar uma base apropriada para a identificação e avaliação dos riscos, e o desenho de procedimentos de auditoria adicionais, pode ser obtida através de indagações junto do órgão de gestão e dos responsáveis pelo relato financeiro.

A23. As indagações junto do órgão de gestão e dos responsáveis pelo relato financeiro e de outras pessoas apropriadas dentro da entidade e a empregados com diferentes níveis hierárquicos, podem oferecer ao auditor perspetivas variadas ao identificar e avaliar os riscos de distorção material.

Exemplos:

- Indagações dirigidas aos encarregados da governação podem ajudar o auditor a compreender o grau de supervisão por parte dos encarregados da governação sobre a preparação das demonstrações financeiras. A ISA 260 (Revista)[23] identifica a importância de uma comunicação eficaz nos dois sentidos para auxiliar o auditor a obter informação dos encarregados da governação a este respeito.
- Indagações a empregados responsáveis pela iniciação, processamento ou registo de transações complexas ou não usuais podem ajudar o auditor a avaliar a apropriação da seleção e aplicação de determinadas políticas contabilísticas.
- Indagações dirigidas ao departamento jurídico interno podem proporcionar informação acerca de matérias como litígios, cumprimento de leis e regulamentos, conhecimento de fraude ou de suspeita de fraude que afete a entidade, garantias, obrigações pós-venda, acordos com parceiros de negócios (tais como empreendimentos conjuntos) e o significado de termos contratuais.
- Indagações dirigidas ao pessoal de marketing ou de vendas podem proporcionar informação acerca de alterações nas estratégias de marketing da entidade, evolução das vendas ou acordos contratuais com os seus clientes.
- Indagações dirigidas à função de gestão de risco (ou indagações aos que executam tal papel) podem proporcionar informação sobre os riscos operacionais e regulamentares que podem afetar o relato financeiro.
- Indagações dirigidas ao pessoal de TI podem proporcionar informação sobre alterações no sistema, falhas no sistema ou nos controlos ou sobre outros riscos associados a TI.

Considerações Específicas Para Entidades do Setor Público

A24. Ao efetuar indagações àqueles que possam ter informações suscetíveis de ajudar a identificar riscos de distorções materiais, os auditores de entidades do sector público podem obter informações de fontes adicionais, tais como dos auditores que estão envolvidos em auditorias de desempenho ou em outras auditorias relacionadas com a entidade.

Indagações à Função de Auditoria Interna

O **Apêndice 4** estabelece orientações para entender a função de auditoria interna de uma entidade

Porque São Efetuadas Indagações Sobre a Função de Auditoria Interna (se a função existe)

A25. Se uma entidade tiver uma função de auditoria interna, as indagações aos indivíduos apropriados dentro dessa função podem auxiliar o auditor no entendimento da entidade e do seu ambiente e do seu sistema de controlo interno, na identificação e avaliação dos riscos.

Considerações Específicas para Entidades do Setor

A26. Os auditores de entidades do setor público têm, muitas vezes, responsabilidades adicionais relativamente ao controlo interno e ao cumprimento de leis e regulamentos aplicáveis. As indagações aos indivíduos apropriados dentro da função de auditoria interna podem auxiliar os auditores a identificar o risco material de incumprimento de leis e regulamentos aplicáveis e o risco de existirem deficiências de controlo relacionadas com o relato

[23] ISA 260 (Revista), *Comunicação com os Encarregados da Governação*, parágrafo 4(b)

financeiro.

Procedimentos Analíticos (Ref: Parágrafo 14(b))

Porque São Efetuados Procedimentos Analíticos como um Procedimento de Avaliação do Risco

A27. Os procedimentos analíticos ajudam a identificar inconsistências. a existência de transações ou acontecimentos não usuais e de quantias, rácios e tendências que indicam matérias que podem ter implicações na auditoria. Relacionamentos não usuais ou inesperados que sejam identificados podem ajudar o auditor na identificação de riscos de distorção material, especialmente riscos de distorção material devido a fraude.

A28. Os procedimentos analíticos executados como procedimentos de avaliação do risco podem assim auxiliar na identificação e avaliação dos riscos de distorção material ao identificar aspetos da entidade os quais o auditor desconhecia ou a compreender como os fatores de risco inerente, tais como alterações, afetam a suscetibilidade da asserção ao risco.

Tipos de Procedimentos Analíticos

A29. Procedimentos analíticos realizados como procedimentos de avaliação de risco podem:

- Incluir informação financeira e não financeira, por exemplo, a relação entre vendas e metros quadrados de espaço de venda ou volume de bens vendidos (não financeiros).
- Utilizar dados agregados a um nível mais elevado. Consequentemente, os resultados desses procedimentos analíticos podem proporcionar os primeiros sinais gerais sobre a probabilidade de distorção material.

Exemplo:

Numa auditoria a muitas entidades, incluindo aquelas com modelos e processos de negócio menos complexos, e um sistema de informação menos complexo, o auditor pode efetuar uma simples comparação de informações, tais como a variação dos saldos intercalares ou mensais face aos saldos de períodos anteriores, para obter uma indicação de áreas de risco potencialmente mais elevado.

A30. Esta norma trata da utilização pelo auditor de procedimentos analíticos como procedimentos de avaliação de riscos. A ISA 520[24] trata da utilização pelo auditor de procedimentos analíticos como procedimentos substantivos ("procedimentos analíticos substantivos") e da responsabilidade do auditor em executar procedimentos analíticos perto do fim da auditoria. Consequentemente, procedimentos analíticos efetuados como procedimentos de avaliação dos riscos não são necessários ser executados de acordo com os requisitos da ISA 520. Todavia, os requisitos e o material de aplicação da ISA 520 podem proporcionar orientações úteis ao auditor aquando da realização de procedimentos analíticos no âmbito dos procedimentos de avaliação do risco.

Ferramentas e técnicas automatizadas

A31. Os procedimentos analíticos podem ser realizados usando uma série de ferramentas ou técnicas, que podem ser automatizadas. A aplicação de procedimentos analíticos automatizados aos dados pode ser referida como análise de dados.

Exemplo:

O auditor pode utilizar uma folha de cálculo para efetuar uma comparação das quantias registadas reais com quantias orçamentadas, ou pode efetuar um procedimento mais avançado através da extração de dados do sistema de informação da entidade, e analisar ainda mais estes dados utilizando técnicas de visualização para identificar classes de transações, saldos de contas ou divulgações para as quais se possa justificar a realização de procedimentos específicos adicionais de avaliação de risco.

Observação e Inspeção (Ref: Parágrafo 14(c))

Por que razão a Observação e a Inspeção São Realizadas como Procedimentos de Avaliação de Risco

A32. A observação e a inspeção podem apoiar, corroborar ou contradizer indagações ao órgão de gestão e a outros, e também podem proporcionar informações sobre a entidade e o seu ambiente.

[24] ISA 520, *Procedimentos analíticos*

Escalabilidade

A33. Quando as políticas ou procedimentos não forem documentados, ou a entidade tiver controlos menos formalizados, o auditor poderá ainda assim obter alguma prova de auditoria que suporte a identificação e avaliação dos riscos de distorção material através da observação ou inspeção do desempenho do controlo.

Exemplos:

- O auditor pode obter uma compreensão dos controlos sobre uma contagem de inventários, mesmo que não tenham sido documentados pela entidade, através de observação direta.
- O auditor pode observar a segregação de funções.
- O auditor poderá observar a introdução de palavras-passe.

Observação e Inspeção como Procedimentos de Avaliação de Risco

A34. Os procedimentos de avaliação do risco podem incluir observação ou inspeção do seguinte:

- Operações da entidade.
- Documentos internos (tais como planos de negócios e estratégias), registos e manuais de controlo interno.
- Relatórios elaborados pelo órgão de gestão (tais como relatórios de gestão trimestrais e demonstrações financeiras intercalares) e pelos responsáveis pela governação (tais como atas de reuniões do Conselho de Administração).
- Locais e instalações fabris da entidade.
- Informações obtidas a partir de fontes externas, como revistas comerciais e económicas; relatórios de analistas, bancos ou agências de rating; publicações regulamentares ou financeiras; ou outros documentos externos sobre o desempenho financeiro da entidade (tais como os referidos no parágrafo A79).
- Comportamentos e ações da gestão ou dos responsáveis pela governação (como a observação de uma reunião do comité de auditoria).

Ferramentas e técnicas automatizadas

A35. Ferramentas ou técnicas automatizadas também podem ser usadas para observar ou inspecionar, nomeadamente ativos, por exemplo através da utilização de ferramentas de observação remotas (ex: um drone).

Considerações Específicas para Entidades do Sector Público

A36. Os procedimentos de avaliação dos riscos efetuados por auditores de entidades do sector público também podem incluir a observação e a inspeção dos documentos elaborados pelo órgão de gestão destinados aos órgãos legislativos, por exemplo documentos relacionados com obrigações de relato de desempenho.

Informações de Outras Fontes (Ref: Parágrafo 15)

Por que razão o Auditor Considera Informações de Outras Fontes

A37. Informações obtidas de outras fontes podem ser relevantes para a identificação e avaliação dos riscos de distorção material, ao proporcionarem informações e perceções sobre:

- A natureza da entidade e os seus riscos de negócio, e o que pode ter alterado desde os períodos anteriores.
- A integridade e os valores éticos do órgão de gestão e dos responsáveis pela governação, que também podem ser relevantes para a compreensão do auditor sobre o ambiente de controlo.
- O referencial de relato financeiro aplicável e a sua aplicação à natureza e circunstâncias da entidade.

Outras Fontes Relevantes

A38. Outras fontes de informação relevantes incluem:

- Os procedimentos do auditor relativos à aceitação ou continuação da relação com o cliente ou ao trabalho de auditoria em conformidade com a ISA 220 (Revista), incluindo as conclusões que aí resultaram.[25]
- Outros trabalhos realizados para a entidade pelo sócio responsável pela auditoria. O sócio responsável pela auditoria pode ter obtido conhecimentos relevantes para a auditoria, incluindo sobre a entidade e o seu ambiente, ao executar outros trabalhos para a entidade. Esses trabalhos podem incluir trabalhos de acordados ou outros trabalhos de auditoria ou de garantia de fiabilidade, incluindo trabalhos para responder aos requisitos adicionais de relato na jurisdição.

Informações resultantes da Experiência Prévia do Auditor com a Entidade e de Auditorias Anteriores (Ref: Parágrafo 16)

Por que razão as informações de auditorias anteriores são importantes para a auditoria atual

A39. A experiência anterior do auditor com a entidade e os procedimentos de auditoria efetuados em auditorias anteriores podem proporcionar ao auditor informações relevantes para a determinação pelo auditor da natureza e extensão dos procedimentos de avaliação do risco, bem como identificação e avaliação dos riscos de distorção material.

Natureza das Informações de Auditorias Anteriores

A40. A experiência anterior do auditor com a entidade e os procedimentos de auditoria efetuados em auditorias anteriores podem proporcionar ao auditor informações sobre matérias como:

- Distorções passadas e se foram corrigidas em tempo oportuno.
- A natureza da entidade e o seu ambiente, bem como o sistema de controlo interno da entidade (incluindo deficiências de controlo).
- Alterações significativas que a entidade ou as suas operações possam ter sofrido desde o período financeiro anterior.
- Tipos específicos de transações e outros acontecimentos ou saldos de contas (e divulgações relacionadas) em que o auditor sentiu dificuldades em executar os procedimentos de auditoria necessários, por exemplo, devido à sua complexidade.

A41. É exigido ao auditor que determine se as informações obtidas a partir da experiência anterior do auditor com a entidade e dos procedimentos de auditoria efetuados em auditorias anteriores permanecem relevantes e fiáveis, se o auditor planeia utilizar essa informação para efeitos da auditoria em curso. Se a natureza ou circunstâncias da entidade tiverem mudado ou se tiverem sido obtidas novas informações, as informações de períodos anteriores podem deixar de ser relevantes ou fiáveis para a auditoria em curso. Para determinar se ocorreram alterações que possam afetar a relevância ou a fiabilidade dessas informações, o auditor pode efetuar indagações e executar outros procedimentos de auditoria adequados, tais como tais como análises de funcionamento (*walk-throughs)* de sistemas relevantes. Se as informações não forem fiáveis, o auditor pode considerar a realização de procedimentos adicionais adequados nas circunstâncias.

Discussões da Equipa de Trabalho (Ref: Parágrafo. 17-18)

Por que razão se Exige que a Equipa de trabalho Discuta a Aplicação da do Referencial de Relato Financeiro Aplicável e a Suscetibilidade das Demonstrações Financeiras da Entidade a Distorções Materiais

A42. A discussão no seio da equipa de trabalho sobre a aplicação do referencial de relatos financeiro aplicável e a suscetibilidade das demonstrações financeiras da entidade a distorções materiais:

- Proporciona uma oportunidade para que membros da equipa de trabalho mais experientes, incluindo o sócio responsável pelo trabalho, partilhem as suas ideias com base no seu conhecimento da entidade. A partilha de informação contribui para uma compreensão reforçada por todos os membros da equipa de trabalho.
- Permite que os membros da equipa de trabalho troquem informações sobre os riscos de negócio a que a entidade está sujeita, como os fatores de risco inerente podem afetar a suscetibilidade a distorção das classes de transações, saldos de contas e divulgações, e sobre como e onde as demonstrações financeiras podem ser suscetíveis a distorções materiais devido a fraude ou erro.
- Ajuda os membros da equipa de trabalho a compreender melhor o potencial de distorção material das

[25] ISA 220 (Revista), *Gestão da Qualidade para uma Auditoria de Demonstrações Financeiras,* parágrafos 22 a 24

demonstrações financeiras nas áreas específicas que lhes são atribuídas, e a compreender como os resultados dos procedimentos de auditoria que realizam podem afetar outros aspetos da auditoria, incluindo as decisões sobre a natureza, oportunidade e extensão de procedimentos de auditoria adicionais. Em particular, a discussão ajuda os membros da equipa de trabalho a considerarem informações contraditórias baseadas no entendimento que cada membro tem sobre a natureza e as circunstâncias da entidade.

- Proporciona uma base sobre a qual os membros da equipa de trabalho comunicam e partilham novas informações obtidas ao longo da auditoria que podem afetar a avaliação dos riscos de distorção material ou os procedimentos de auditoria realizados para fazer face a estes riscos.

A ISA 240 exige que a discussão da equipa de envolvimento coloque especial ênfase na forma como e onde as demonstrações financeiras da entidade podem ser suscetíveis a distorção material devido a fraude, incluindo a forma como a fraude pode ocorrer.[26]

A43. O ceticismo profissional é necessário para a avaliação crítica da de prova de auditoria, e uma discussão robusta e aberta da equipa de trabalho, incluindo para auditorias recorrentes, pode levar a uma melhor identificação e avaliação dos riscos de distorção material. Outro resultado da discussão poderá ser o auditor identificar áreas específicas da auditoria para as quais o exercício do ceticismo profissional pode ser particularmente importante, podendo conduzir ao envolvimento de membros mais experientes da equipa de trabalho que são devidamente qualificados para serem envolvidos na realização dos procedimentos de auditoria relacionados com essas áreas.

Escalabilidade

A44. Quando o trabalho for efetuado por um único indivíduo, como no caso em que o auditor exerce a atividade a título individual (isto é, quando não seria possível uma discussão em equipa de trabalho), a análise das matérias referidas nos parágrafos A42 e A46 pode, no entanto, ajudar o auditor a identificar quando pode haver riscos de distorção material.

A45. Quando um trabalho é realizado por uma grande equipa de trabalho, como por exemplo, uma auditoria às demonstrações financeiras do grupo, nem sempre é necessário ou prático que a discussão inclua todos os membros numa única discussão (por exemplo, numa auditoria em múltiplos locais), nem é necessário que todos os membros da equipa de trabalho sejam informados de todas as decisões tomadas na discussão. O sócio responsável pelo trabalho pode discutir assuntos com membros-chave da equipa de trabalho, incluindo, se considerado adequado, aqueles com competências ou conhecimentos específicos, e aqueles que são responsáveis pelo trabalho a ser realizado nas componentes, e delegar a discussão com outros, tendo em conta a extensão da comunicação considerada necessária com toda a equipa de trabalho. Um plano de comunicações, acordado pelo sócio responsável pelo compromisso, pode ser útil.

Discussão de Divulgações no Referencial de Relato Financeiro Aplicável

A46. No âmbito da discussão no seio da equipa de trabalho, a análise dos requisitos de divulgação do referencial de relato financeiro aplicável ajuda a identificar na fase inicial da auditoria onde podem existir riscos de distorção material em relação às divulgações, mesmo em circunstâncias em que o referencial de relato financeiro aplicável apenas exija divulgações simplificadas. Os assuntos que a equipa de trabalho pode discutir incluem:

- Alterações nos requisitos de relato financeiro que possam resultar em divulgações novas ou revistas significativas;
- Alterações no ambiente, condição financeira ou atividades da entidade que possam resultar em divulgações novas ou revistas significativas, por exemplo, uma combinação de negócios significativa no período abrangido pela auditoria;
- Divulgações para as quais a obtenção de prova de auditoria adequada e suficiente pode ter sido difícil no passado;
- Divulgações sobre assuntos complexos, incluindo aqueles que envolvem um julgamento significativo por parte do órgão de gestão sobre que informação divulgar.

Considerações Específicas para Entidades do Sector Público

A47. No âmbito da discussão no seio da equipa de trabalho por parte de auditores de entidades do sector público, também pode ser ponderada atenção a quaisquer objetivos adicionais mais amplos e riscos relacionados, decorrentes do mandato de auditoria ou das obrigações para as entidades do sector público.

[26] ISA 240, parágrafo 16

Obtenção de um Entendimento da Entidade e do Seu Ambiente, d Referencial de Relato Financeiro Aplicável e do Sistema de Controlo Interno da Entidade (Ref: Parágrafo 19-27)

Os **apêndices 1 a 6** apresentam considerações adicionais relativas à obtenção de um entendimento da entidade e do seu ambiente, do referencial de relato financeiro aplicável e do sistema de controlo interno da entidade.

Obtenção do Entendimento Obrigatório (Ref: Parágrafo 19-27)

A48. A obtenção de um entendimento da entidade e do seu ambiente, do referencial de relato financeiro aplicável e do sistema de controlo interno da entidade é um processo dinâmico e iterativo de recolha, atualização e análise de informação que continua ao longo da auditoria. Consequentemente, as expectativas do auditor podem mudar à medida que novas informações são obtidas.

A49. A compreensão do auditor sobre a entidade e o seu ambiente e o referencial de relato financeiro aplicável também pode ajudar o auditor a desenvolver expectativas iniciais sobre as classes de transações, saldos de contas e divulgações que possam ser significativas. Estas esperadas categorias de transações, saldos de contas e divulgações significativas constituem a base para o âmbito da compreensão do auditor sobre o sistema de informação da entidade.

Por que razão é necessária uma Compreensão da Entidade e do Seu Ambiente, e do Referencial de Relato Financeiro Aplicável (Ref: Parágrafo 19-20)

A50. O entendimento do auditor sobre a entidade e do seu ambiente, bem como do referencial de relato financeiro aplicável, ajuda o auditor a compreender os acontecimentos e condições relevantes para a entidade e a identificar como os fatores de risco inerente afetam a suscetibilidade das asserções a distorções na preparação das demonstrações financeiras, de acordo com o referencial de relato financeiro aplicável, e o grau em que o fazem. Estas informações estabelecem um referencial no seio do qual o auditor identifica e avalia os riscos de distorção material. Este referencial também ajuda o auditor no planeamento da auditoria e no exercício do julgamento profissional e do ceticismo profissional ao longo da auditoria, por exemplo, quando:

- Identificar e avaliar os riscos de distorção material das demonstrações financeiras de acordo com a ISA 315 (Revista 2019) ou outras normas relevantes (por exemplo, relativas a riscos de fraude em conformidade com a ISA 240 ou quando identificar ou avaliar riscos relacionados com estimativas contabilísticas em conformidade com a ISA 540 (Revista);
- Executar procedimentos para ajudar a identificar casos de incumprimento de leis e regulamentos que possam ter um efeito material nas demonstrações financeiras de acordo com a ISA 250;[27]
- Avaliar se as demonstrações financeiras proporcionam divulgações adequadas de acordo com a ISA 700 (Revista);[28]
- Determinar a materialidade ou a materialidade de desempenho de acordo com a ISA 320; [29] ou
- Considerar a adequação da seleção e aplicação das políticas contabilísticas, e a adequação das divulgações de demonstrações financeiras.

A51. O entendimento do auditor sobre a entidade e o seu ambiente, bem como o referencial de relato financeiro aplicável, também informa sobre como o auditor planeia e executa procedimentos de auditoria adicionais, por exemplo, quando:

- Desenvolver expectativas para uso ao executar procedimentos analíticos de acordo com a ISA 520;[30]
- Conceber e executar novos procedimentos de auditoria para obter prova de auditoria adequada e suficiente em conformidade com a ISA 330; e
- valiar a suficiência e adequação da prova obtida (por exemplo, relativa a pressupostos ou representações orais e escritas do órgão de gestão).

Escalabilidade

A52. A natureza e extensão do entendimento exigido é uma questão de julgamento profissional do auditor e varia de entidade para entidade com base na natureza e circunstâncias da entidade, incluindo:

---

27 ISA 250 (Revista), *Apreciação de leis e regulamentos numa auditoria de demonstrações financeiras,* parágrafo 14

28 ISA 700 (Revista), *Formação de um parecer e relatórios sobre demonstrações financeiras,* parágrafo 13 e

29 ISA 320, *Materialidade no Planeamento e Realização de uma Auditoria*, parágrafos 10-11

30 ISA 520, parágrafo 5

- O tamanho e complexidade da entidade, incluindo o seu ambiente de TI;
- A experiência anterior do auditor com a entidade;
- A natureza dos sistemas e processos da entidade, incluindo se são formalizados ou não; e
- A natureza e a forma da documentação da entidade.

A53. Os procedimentos de avaliação de risco do auditor para obter o entendimento exigido podem ser menos extensivos em auditorias de entidades menos complexas e mais extensos para entidades mais complexas. Espera-se que a profundidade do entendimento exigido pelo auditor seja inferior àquele que do órgão de gestão possui decorrente de gerir a entidade.

A54. Alguns referenciais de relato financeiro permitem que entidades mais pequenas forneçam divulgações mais simples e menos detalhadas nas demonstrações financeiras. No entanto, tal não alivia o auditor da responsabilidade de obter um entendimento da entidade e do seu ambiente e do referencial de relato financeiro aplicável, tal como se aplica à entidade.

A55. A utilização de TI pela entidade e a natureza e extensão das mudanças no ambiente de TI podem também afetar as competências especializadas que são necessárias para ajudar a obter a compreensão exigida.

A Entidade e o Seu Ambiente (Ref: Parágrafo 19 a)

Estrutura Organizacional, Propriedade e Governação da Entidade e Modelo de Negócio (Ref: Parágrafo 19(a)(i))

Estrutura organizacional e propriedade da entidade

A56. Uma compreensão da estrutura organizacional e da propriedade da entidade pode permitir ao auditor compreender matérias como:

- A complexidade da estrutura da entidade.

Exemplo:

A entidade pode ser uma entidade única ou a estrutura da entidade pode incluir subsidiárias, divisões ou outros componentes em vários locais. Além disso, a estrutura legal pode ser diferente da estrutura operacional. Estruturas complexas introduzem frequentemente fatores que podem dar origem a uma maior suscetibilidade aos riscos de distorção material. Estas matérias podem incluir se o *goodwill*, os empreendimentos conjuntos, os investimentos ou as entidades com finalidade especial são contabilizados apropriadamente e se foram feitas, as divulgações adequadas nas demonstrações financeiras.

- A propriedade, e as relações entre proprietários e outras pessoas ou entidades, incluindo partes relacionadas. Este entendimento pode ajudar a determinar se as transações entre as partes relacionadas foram devidamente identificadas, contabilizadas e adequadamente divulgadas nas demonstrações financeiras.[31]
- A distinção entre os proprietários, os encarregados da governação e o órgão de gestão.

Exemplo:

Em entidades menos complexas, os proprietários da entidade podem estar envolvidos na gestão da entidade, pelo que há pouca ou nenhuma distinção. Em contrapartida, como em algumas entidades cotadas, pode haver uma distinção clara entre o órgão de gestão, os proprietários da entidade e os encarregados da governação.[32]

- A estrutura e complexidade do ambiente de TI da entidade.

Exemplos:

Uma entidade pode:

- Ter múltiplos sistemas de TI antigos em diversos negócios que não estão bem integrados resultando num complexo ambiente de TI.
- Estar a utilizar prestadores de serviços externos ou internos para aspetos do seu ambiente de TI (por

[31] A ISA 550 estabelece requisitos e proporciona orientações sobre as considerações do auditor relevantes para as partes relacionadas.

[32] A ISA 260 (Revista), os parágrafos A1 e A2, proporcionam orientações sobre a identificação dos encarregados da governação e explicam que, em alguns casos, alguns ou todos os encarregados da governação podem estar envolvidos na gestão da entidade.

exemplo, subcontratar o alojamento do seu ambiente de TI a terceiros ou utilizar um centro de serviços partilhados para a gestão central dos processos de TI num grupo).

Ferramentas e técnicas automatizadas

A57. O auditor pode utilizar ferramentas e técnicas automatizadas para compreender os fluxos de transações e o processamento como parte dos procedimentos do auditor para compreender o sistema de informação. Um resultado destes procedimentos pode ser que o auditor obtenha informações sobre a estrutura organizacional da entidade ou sobre aqueles com quem a entidade conduz negócios (por exemplo, fornecedores, clientes, partes relacionadas).

Considerações específicas para entidades do sector público

A58. A propriedade de uma entidade do sector público pode não ter a mesma relevância que no sector privado, uma vez que as decisões relacionadas com a entidade podem ser tomadas fora da entidade em resultado de processos políticos. Consequentemente, o órgão de gestão pode não ter controlo sobre determinadas decisões que são tomadas. As matérias que podem ser relevantes incluem entender a capacidade da entidade para tomar decisões unilaterais, e a capacidade de outras entidades do setor público controlarem ou influenciarem o mandato e a direção estratégica da entidade.

Exemplo:

Uma entidade do sector público pode estar sujeita a leis ou outras diretivas das autoridades que exijam que esta obtenha aprovação de partes externas à entidade acerca da sua estratégia e objetivos antes da sua implementação. Assim, as matérias relacionadas com o entendimento da estrutura legal da entidade podem incluir leis e regulamentos aplicáveis, e a classificação da entidade (ou seja, se a entidade é um ministério, departamento, agência ou outro tipo de entidade).

Governação

Por que razão o auditor obtém um entendimento da governação

A59. Compreender a governação da entidade pode ajudar o auditor a compreender a capacidade da entidade de proporcionar uma supervisão adequada do seu sistema de controlo interno. No entanto, este entendimento também pode proporcionar evidência de deficiências, o que pode indicar um aumento da suscetibilidade das demonstrações financeiras da entidade aos riscos de distorção material.

Compreender a governação da entidade

A60. As matérias que podem ser relevantes para o auditor considerar na obtenção de um entendimento da governação da entidade incluem:

- Se algum ou todos os encarregados da governação estão envolvidos na gestão da entidade.
- A existência de um Conselho Não Executivo, se for caso disso, separado da gestão executiva.
- Se os encarregados da governação ocupam cargos que fazem parte integrante da estrutura legal da entidade, por exemplo, como administradores.
- A existência de subgrupos encarregados da governação, tais como um comité de auditoria, e as responsabilidades de tal grupo.
- As responsabilidades dos encarregados da governação pela supervisão do relato financeiro, incluindo a aprovação das demonstrações financeiras.

Modelo de Negócio da Entidade

O apêndice 1 apresenta considerações adicionais para a obtenção de um entendimento da entidade e do seu modelo de negócio, bem como considerações adicionais para a auditoria de entidades com finalidade especiais.

Por que razão o auditor obtém uma compreensão do modelo de negócio da entidade

A61. Compreender os objetivos, estratégia e modelo de negócio da entidade ajuda o auditor a compreender a entidade a nível estratégico, e a compreender os riscos de negócio que a entidade assume e enfrenta. Uma compreensão dos riscos empresariais que têm um efeito nas demonstrações financeiras ajuda o auditor a

identificar riscos de distorção material, uma vez que a maioria dos riscos empresariais acabará por ter consequências financeiras e, portanto, um efeito nas demonstrações financeiras.

Exemplos:

O modelo de negócio de uma entidade pode contar com a utilização de TI de diferentes formas:

- A entidade vende sapatos a partir de uma loja física, e usa um sistema avançado de *stock*s e ponto de venda para registar a venda de sapatos; ou
- A entidade vende sapatos *online* para que todas as transações de vendas sejam processadas num ambiente de TI, incluindo o início das transações através de um *website*.

Para ambas as entidades, os riscos de negócio decorrentes de um modelo de negócio significativamente diferente seriam substancialmente diferentes, não obstante ambas as entidades venderem calçado.

Compreender o modelo de negócio da entidade

A62. Nem todos os aspetos do modelo de negócio são relevantes para o entendimento do auditor. Os riscos de negócio são mais amplos do que os riscos de distorção material das demonstrações financeiras, embora os riscos negócio incluam estes últimos. O auditor não tem a responsabilidade de entender ou identificar todos os riscos de negócio, porque nem todos os riscos de negócio dão origem a riscos de distorção material.

A63. Os riscos de negócio aumentarem a suscetibilidade aos riscos de distorção material podem resultar de:

- Objetivos ou estratégias inadequadas, execução ineficaz de estratégias, ou alteração ou complexidade.
- Falha no reconhecimento da necessidade de mudança pode também dar origem a riscos de negócio, por exemplo, a partir:
  - Do desenvolvimento de novos produtos ou serviços que podem fracassar;
  - De um mercado que, mesmo que desenvolvido com sucesso, é inadequado para suportar um produto ou serviço;
  - De defeitos num produto ou serviço que podem resultar em responsabilidade legal e risco de reputação.
- Incentivos e pressões sobre o órgão de gestão, que podem resultar em enviesamentos do órgão de gestão intencionais ou não intencionais, e, portanto, afetar a razoabilidade de pressupostos significativos e as expectativas do órgão de gestão ou dos encarregados da governação.

A64. Exemplos de matérias que o auditor pode considerar ao obter um entendimento do modelo de negócio da entidade, objetivos, estratégias e riscos negócio relacionados que possam resultar num risco de distorção material das demonstrações financeiras incluem:

- Desenvolvimentos da indústria, como a falta de pessoal ou conhecimentos especializados para lidar com as mudanças no setor;
- Novos produtos e serviços que podem levar a um aumento de passivos do produto;
- Expansão do negócio da entidade e em que a procura não tenha sido estimada com rigor;
- Novos requisitos contabilísticos em que tenha havido uma implementação incompleta ou inadequada;
- Requisitos regulamentares que resultem num aumento da exposição legal;
- Requisitos de financiamento correntes e potenciais, tais como perda de financiamento devido à incapacidade da entidade em satisfazer os requisitos;
- Utilização de TI, como a implementação de um novo sistema de TI que afetará tanto as operações como o relato financeiro; ou
- Os efeitos da implementação de uma estratégia, particularmente quaisquer efeitos que conduzam a novos requisitos contabilísticos.

A65. Normalmente, o órgão de gestão identifica os riscos de negócio e desenvolve abordagens para os resolver. Este processo de avaliação de riscos faz parte do sistema de controlo interno da entidade e é discutido no parágrafo 22 e nos parágrafos A109-A113.

Considerações específicas para entidades do sector público

A66. As entidades que operam no sector público podem criar e entregar valor de diferentes formas a quem cria riqueza para os proprietários, mas continuará a ter um "modelo de negócio" com um objetivo específico. As matérias sobre as quais os auditores do sector público podem obter um entendimento e que são relevantes para o modelo de negócio da entidade, incluem:

- Conhecimento das atividades governamentais relevantes, incluindo programas relacionados.
- Objetivos programáticos e estratégias, incluindo elementos de política pública.

A67. Para as auditorias de entidades do sector público, os "objetivos da gestão" podem ser influenciados por requisitos para demonstrar responsabilidade pública e podem incluir objetivos que tenham a sua fonte na lei, regulamentos ou outra autoridade.

Indústria, Regulamentação e Outros Fatores Externos (Ref: Parágrafo 19(a)(ii))

Fatores da indústria

A68. Os fatores relevantes da indústria incluem condições da indústria, tais como o ambiente competitivo, as relações com fornecedores e clientes, e a evolução tecnológica. As matérias que o auditor pode considerar incluem:

- Mercado e concorrência, incluindo procura, capacidade e concorrência de preços.
- Atividade cíclica ou sazonal.
- Tecnologia dos produtos relativa aos produtos da entidade.
- Fornecimento de energia e custo.

A69. A indústria em que a entidade opera pode dar origem a riscos específicos de distorção material decorrentes da natureza da atividade ou do grau de regulamentação.

> **Exemplo**:
>
> No sector da construção, os contratos de longo prazo podem implicar estimativas significativas de receitas e despesas que dão origem a riscos de distorção material. Nestes casos, é importante que a equipa de trabalho inclua membros com conhecimento e experiência suficientes.[33]

Fatores regulamentares

A70. Os fatores regulamentares relevantes incluem o ambiente regulamentar. O ambiente regulamentar engloba, entre outras matérias, o referencial de relato financeiro aplicável e o ambiente jurídico e político e quaisquer alterações daí resultantes. As matérias que o auditor pode considerar incluem:

- O referencial regulamentar para uma indústria regulamentada, por exemplo, requisitos prudenciais, incluindo divulgações relacionadas.
- Legislação e regulamentação que afetam significativamente as operações da entidade, por exemplo, leis e regulamentos laborais.
- Legislação e regulamentos fiscais.
- As políticas governamentais que à data afetam a condução dos negócios da entidade, tais como as monetárias, incluindo controlos cambiais, incentivos fiscais, financeiros (por exemplo, programas de ajuda governamental) e tarifas ou políticas de restrição comercial.
- Requisitos ambientais que afetam a indústria e o negócio da entidade.

A71. A ISA 250 (Revista) inclui alguns requisitos específicos relacionados com o referencial legal e regulamentar aplicável à entidade e à indústria ou sector em que a entidade opera.[34]

Considerações específicas para entidades do sector público

A72. Para as auditorias de entidades do sector público, pode haver leis ou regulamentos específicos que afetem as operações da entidade. Tais elementos podem ser uma consideração essencial quando se obtém um entendimento da entidade e do seu ambiente.

---

[33] ISA 220 (Revista), parágrafos 25 a 28
[34] ISA 250 (Revista), parágrafo 13

Outros fatores externos

A73. Outros fatores externos que afetam a entidade e que o auditor pode considerar incluem as condições económicas gerais, as taxas de juro e a disponibilidade de financiamento, bem como a inflação ou a revalorização monetária.

Medidas Usadas pela Órgão de Gestão para Avaliar o Desempenho Financeiro da Entidade (Ref: Parágrafo 19 a(iii))

Por que razão o auditor compreende as medidas usadas pelo órgão de gestão

A74. entendimento compreensão das medidas da entidade ajuda o auditor a considerar se tais medidas, usadas externa ou internamente, criam pressões sobre a entidade para atingir objetivos de desempenho. Estas pressões podem motivar a o órgão de gestão a tomar medidas que aumentem a suscetibilidade a distorção devido a enviesamentos do órgão de gestão ou fraude (por exemplo, para melhorar o desempenho do negócio ou para distorcer intencionalmente as demonstrações financeiras) (ver a ISA 240 para requisitos e orientações em relação aos riscos de fraude).

A75. As medidas também podem dar indicações ao auditor da probabilidade de riscos de distorção material nas informações constantes da demonstração financeira relacionada. Por exemplo, as medidas de desempenho podem indicar que a entidade tem um crescimento ou rentabilidade invulgarmente rápidos quando comparadas com as de outras entidades da mesma indústria.

Medidas usadas pelo órgão de gestão

A76. O órgão de gestão e outros normalmente medem e revêm as matérias que consideram importantes. As indagações ao órgão de gestão podem revelar que esta se baseia em certos indicadores-chave, disponíveis ou não publicamente, para avaliar o desempenho financeiro e tomar medidas. Nesses casos, o auditor pode identificar medidas de desempenho relevantes, internas ou externas, tendo em conta as informações que a entidade utiliza para gerir o seu negócio. Se tal indagação indicar uma ausência de medição ou revisão do desempenho, pode haver um risco acrescido de as distorções não serem detetadas e corrigidas.

A77. Os principais indicadores utilizados para avaliar o desempenho financeiro podem incluir:

- Principais indicadores de desempenho (financeiros e não financeiros) e rácios-chave, tendências e estatísticas operacionais.
- Análises comparativas de desempenho financeiro entre períodos.
- Orçamentos, previsões, análises de variância, informações por segmentos e relatórios de desempenho por divisão, departamentos ou outros níveis.
- Medidas de desempenho dos colaboradores e políticas de remuneração com incentivos.
- Comparações do desempenho de uma entidade com o desempenho dos concorrentes.

Escalabilidade (Ref: Parágrafo 19 (a) (iii))

A78. Os procedimentos empreendidos para entender as medidas da entidade podem variar consoante a dimensão ou complexidade da entidade, bem como o envolvimento dos proprietários ou dos encarregados da governação na gestão da entidade.

Exemplos:

- Para algumas entidades menos complexas, os termos dos empréstimos bancários da entidade (isto é, os contratos bancários) podem estar ligados a medidas de desempenho específicas relacionadas com o desempenho ou a situação financeira da entidade (por exemplo, uma quantia máximo de fundo de maneio). O entendimento do auditor sobre as medidas de desempenho usadas pelo banco pode ajudar a identificar áreas em que haja uma maior suscetibilidade ao risco de distorção material.
- Para algumas entidades cuja natureza e circunstâncias sejam mais complexas, como as que operam nas indústrias seguradoras ou bancárias, o desempenho ou a posição financeira podem ser medidos em relação aos requisitos regulamentares (por exemplo, obstáculos ao desempenho em relação a requisitos de rácio regulamentares, como a adequação do capital próprio e os rácios de liquidez). A compreensão do auditor sobre estas medidas de desempenho pode ajudar a identificar áreas em que há uma maior suscetibilidade ao risco de distorção material.

Considerações adicionais

A79. OS parceiros externos também podem rever e analisar o desempenho financeiro da entidade, nomeadamente nas entidades onde a informação financeira está disponível publicamente. O auditor também pode considerar informações disponíveis publicamente, para o ajudar a compreender melhor o negócio ou identificar informações contraditórias, tais como informação de:

- Analistas ou agências de crédito.
- Notícias e outros meios de comunicação, incluindo redes sociais.
- Autoridades fiscais.
- Reguladores.
- Sindicatos.
- Financiadores.

Estas informações financeiras podem frequentemente ser obtidas a partir da entidade que está a ser auditada.

A80. A medição e revisão do desempenho financeiro não é a mesma que a monitorização do sistema de controlo interno (discutida como componente do sistema de controlo interno nos parágrafos A114-A122), embora os seus objetivos possam sobrepor-se:

- A medição e revisão do desempenho é direcionada para saber se o desempenho do negócio está a cumprir os objetivos definidos pelo órgão de gestão (ou por terceiros).
- Em contrapartida, a monitorização do sistema de controlo interno está relacionada com a monitorização da eficácia dos controlos, incluindo os relacionados com a medição da gestão e revisão do desempenho financeiro por parte do órgão de gestão.

Em alguns casos, no entanto, os indicadores de desempenho também proporcionam informações que permitem ao órgão de gestão identificar deficiências de controlo.

Considerações específicas para entidades do sector público

A81. Para além de considerarem medidas relevantes usadas por uma entidade do sector público para avaliar o desempenho financeiro da entidade, os auditores de entidades do sector público podem ainda considerar informações não financeiras, como os resultados de benefícios públicos atingidos (por exemplo, o número de pessoas assistidas por um programa específico).

O Referencial de Relato Financeiro aplicável (Ref: Parágrafo 19 (b))

Compreender o Referencial de Relato Financeiro Aplicável e as Políticas Contabilísticas da Entidade

A82. As matérias que o auditor pode considerar ao obter um entendimento do referencial de relato financeiro aplicável da entidade e como se aplica no contexto da natureza e circunstâncias da entidade e do seu ambiente incluem:

- As práticas de relato financeiro da entidade em termos do referencial de relato financeiro aplicável, tais como:
  - Princípios contabilísticos e práticas específicas do sector, incluindo as relativas a classes de transações específicas do sector significativas, a saldos de contas específicos do sector significativas e divulgações relacionadas nas demonstrações financeiras (por exemplo, empréstimos e investimentos no caso dos bancos, ou investigação e desenvolvimento no caso de produtos farmacêuticos).
  - Reconhecimento do rédito.
  - Contabilização de instrumentos financeiros, incluindo perdas de crédito relacionadas.
  - Ativos, passivos e transações em moeda estrangeira.
  - Contabilização de transações não usuais ou complexas, incluindo as de áreas controversas ou emergentes (por exemplo, contabilização de cripto moeda).
- Uma compreensão da seleção e aplicação das políticas contabilísticas feitas pela entidade, incluindo quaisquer alterações que daí resultem bem como os motivos, pode abranger matérias como:

- Os métodos que a entidade utiliza para reconhecer, medir, apresentar e divulgar transações significativas e não usuais.
- O efeito de políticas contabilísticas significativas em áreas controversas ou emergentes para as quais há falta de orientação ou consenso vinculativo.
- Alterações no ambiente, tais como alterações no referencial de relato financeiro aplicável ou reformas fiscais que podem exigir uma mudança nas políticas contabilísticas da entidade.
- Normas de relato financeiro e Leis e regulamentos que sejam novos para a entidade e quando e como a entidade irá adotar, ou cumprir, esses requisitos.

A83. A obtenção de um conhecimento da entidade e do seu ambiente pode ajudar o auditor a considerar onde podem ser esperadas alterações no relato financeiro da entidade (por exemplo, tendo como ponto de partida períodos anteriores).

> **Exemplo**:
>
> Se a entidade tiver tido uma combinação de negócios significativa durante o período, o auditor provavelmente esperaria alterações nas classes de transações, saldos de contas e divulgações associadas a essa combinação de negócios. Em alternativa, se não se registaram alterações significativas no referencial de relato financeiro durante o período, o parecer do auditor poderá ajudar a confirmar que o entendimento obtido no período anterior permanece aplicável.

Considerações específicas para entidades do sector público

A84. O referencial de informação financeira aplicável numa entidade do sector público é determinado pelos referenciais legislativos e regulamentares relevantes para cada jurisdição ou em cada área geográfica. As matérias que podem ser tidas em conta na aplicação, por parte da entidade, dos requisitos de relato financeiro aplicáveis e na forma como de aplicação no contexto da natureza e circunstância da entidade e do seu ambiente, incluem se a entidade aplica na sua totalidade uma base de contabilística de acréscimo ou uma base contabilística de caixa, de acordo com as Normas Internacionais de Contabilidade do Sector Público, ou um modelo híbrido.

Como os fatores de risco inerente afetam a suscetibilidade das asserções a distorções (Ref: Parágrafo 19(c))

> **O apêndice 2** proporciona exemplos de acontecimentos e condições que podem dar origem à existência de riscos de distorção material, categorizados por fator de risco inerente.

Por que razão o auditor compreende os fatores de risco inerente aquando da compreensão da entidade e do seu ambiente e do quadro de relato financeiro aplicável

A85. A compreensão da entidade e do seu ambiente, e do referencial de relato financeiro aplicável, ajuda o auditor na identificação de acontecimentos ou condições cujas características podem afetar a suscetibilidade de asserções sobre classes de transações, saldos de contas ou divulgações a distorções. Estas características são fatores de risco inerente. Os fatores de risco inerente podem afetar a suscetibilidade das asserções a distorção, influenciando a probabilidade de ocorrência de uma distorção ou a magnitude da distorção caso esta ocorra. Compreender como os fatores de risco inerente afetam a suscetibilidade das asserções distorção pode ajudar o auditor a compreender preliminarmente a probabilidade ou a magnitude das distorções, o que ajuda o auditor a identificar os riscos de distorção material ao nível da asserção, em conformidade o parágrafo 28(b). A compreensão do grau em que os fatores de risco inerente afetam a suscetibilidade das asserções a distorção também ajuda o auditor a avaliar a probabilidade e a magnitude de uma eventual distorção quando avaliar o risco inerente em conformidade com o parágrafo 31(a). Consequentemente, a compreensão dos fatores de risco inerente pode igualmente ajudar o auditor a conceber e a executar procedimentos de auditoria adicionais em conformidade com a ISA 330.

A86. A identificação do auditor dos riscos de distorção materiais ao nível da asserção e a avaliação do risco inerente também podem ser influenciadas por prova de auditoria obtida pelo auditor na realização de outros procedimentos de avaliação de riscos, de procedimentos de auditoria adicionais ou no cumprimento de outros requisitos nas ISA (ver parágrafos A95, A103, A111, A121, A124 e A151).

O efeito dos fatores de risco inerente em classe de transações, saldo de conta ou divulgação

A87. A extensão da suscetibilidade de uma classe de transações, saldo de contas ou divulgação a distorção decorrente

da complexidade ou da subjetividade está muitas vezes intimamente relacionada com a extensão em que está sujeita a alterações ou incertezas.

Exemplo:

Se a entidade tiver uma estimativa contabilística baseada em pressupostos, cuja seleção está sujeita a um julgamento significativo, a mensuração da estimativa contabilística é suscetível de ser afetada tanto pela subjetividade como pela incerteza.

A88. Quanto maior é a extensão em que uma classe de transações, saldo de conta ou divulgação é suscetível a distorção devido à complexidade ou subjetividade, maior é a necessidade de o auditor aplicar o ceticismo profissional. Além disso, quando uma classe de transações, saldo de conta ou divulgação é suscetível a uma distorção devido à complexidade, subjetividade, mudança ou incerteza, estes fatores de risco inerente podem criar oportunidades para enviesamento por parte do órgão de gestão, quer não intencionais quer intencionais, e afetar a suscetibilidade a distorção devido a enviesamentos do órgão de gestão. A identificação do auditor dos riscos de distorção material e a avaliação do risco inerente ao nível da asserção também são afetadas pelas inter-relações entre os fatores de risco inerente.

A89. Acontecimentos ou condições que podem afetar a suscetibilidade a distorção devido a enviesamentos do órgão de gestão também podem afetar a suscetibilidade a distorção devido a outros fatores de risco de fraude. Consequentemente, estas podem ser informações relevantes para utilização em conformidade com o parágrafo 24 da ISA 240, o qual requer que o auditor avalie se as informações obtidas a partir dos outros procedimentos de avaliação do risco e atividades relacionadas indicam a presença de um ou mais fatores de risco de fraude.

Compreender os Componentes do Sistema de Controlo Interno da Entidade (Ref: Parágrafo 21-27)

O apêndice 3 descreve ainda a natureza do sistema de controlo interno da entidade e as limitações inerentes ao controlo interno, respetivamente. O apêndice 3 também proporciona explicação adicional dos componentes de um sistema de controlo interno para efeitos das ISA.

A90. A compreensão do auditor sobre o sistema de controlo interno da entidade é obtida através de procedimentos de avaliação dos riscos, realizados para compreender e avaliar cada um dos componentes do sistema de controlo interno tal como estabelecido nos parágrafos 21 a 27.

A91. Os componentes do sistema de controlo interno da entidade para efeitos desta ISA podem não refletir necessariamente a forma como uma entidade concebe, implementa e mantém o seu sistema de controlo interno, ou a forma como pode classificar qualquer componente específico. As entidades podem utilizar terminologias ou referenciais diferentes para descrever os vários aspetos do sistema de controlo interno. Para efeitos de auditoria, os auditores também podem utilizar terminologias ou referenciais diferentes, desde que sejam abordados todos os componentes descritos nesta ISA.

Escalabilidade

A92. A forma como o sistema de controlo interno da entidade é concebido, implementado e mantido varia com o tamanho e complexidade de uma entidade. Por exemplo, entidades menos complexas podem utilizar controlos menos estruturados ou mais simples (isto é, políticas e procedimentos) para atingir os seus objetivos.

Considerações Específicas para Entidades do Sector Público

A93. Os auditores de entidades do sector público têm muitas vezes responsabilidades adicionais no que diz respeito ao controlo interno, por exemplo, reportar sobre o cumprimento de um código de conduta estabelecido ou reportar sobre as despesas em comparação com o orçamento. Os auditores de entidades do sector público podem ainda ter responsabilidades de relatar sobre o cumprimento da lei, regulamentos ou outra autoridade. Consequentemente, as suas considerações sobre o sistema de controlo interno podem ser mais amplas e mais pormenorizadas.

Tecnologias de Informação nos Componentes do Sistema de Controlo Interno da Entidade

O apêndice 5 proporciona orientações adicionais para a compreensão da forma como a entidade utiliza os TI nos componentes do sistema de controlo interno.

A94. O objetivo geral e o âmbito de uma auditoria não diferem se uma entidade opera num ambiente essencialmente manual, num ambiente completamente automatizado ou num ambiente que envolva alguma combinação de

elementos manuais e automatizados (isto é, controlos manuais e automatizados e outros recursos utilizados no sistema de controlo interno da entidade).

Compreender a Natureza dos Componentes do Sistema de Controlo Interno da Entidade

A95. Ao avaliar a eficácia da conceção dos controlos e se foram implementados (ver parágrafos A175 a A181), a compreensão do auditor sobre cada um dos componentes do sistema de controlo interno da entidade proporciona uma compreensão preliminar de como a entidade identifica os riscos de negócio e como responde aos mesmos. Também pode influenciar, de diferentes formas, a identificação e avaliação dos riscos de distorção material feitas pelo auditor (ver parágrafo A86). Isto ajuda o auditor na conceção e execução de procedimentos de auditoria adicionais, incluindo quaisquer planos para testar a eficácia operacional dos controlos. Por exemplo:

- A compreensão do auditor sobre o ambiente de controlo da entidade, sobre o processo de avaliação de risco da entidade e sobre o processo da entidade para monitorizar os componentes dos controlos são mais suscetíveis de afetar a identificação e avaliação dos riscos de distorção material ao nível da demonstração financeira.
- A compreensão do auditor sobre o sistema de informação e comunicação da entidade, bem como a componente das atividades de controlo da entidade, são mais suscetíveis de afetar a identificação e avaliação dos riscos de distorção material ao nível da asserção.

Ambiente de Controlo, Processo de Avaliação de Riscos da Entidade e Processo da Entidade para Monitorizar o Sistema de Controlo Interno (Ref: Parágrafo 21-24)

A96. Os controlos no ambiente de controlo, o processo de avaliação de riscos da entidade e o processo da entidade para monitorizar o sistema de controlo interno são principalmente controlos indiretos (isto é, controlos que não são suficientemente precisos para prevenir, detetar ou corrigir distorções ao nível da asserção, mas que suportam outros controlos e podem, portanto, ter um efeito indireto na probabilidade de uma distorção vir a ser detetada ou prevenida atempadamente). No entanto, alguns controlos dentro destes componentes podem também ser controlos diretos.

Por que razão se exige ao auditor que compreenda o ambiente de controlo, o processo de avaliação de risco da entidade e o processo da entidade para monitorizar o sistema de controlo interno

A97. O ambiente de controlo proporciona uma base global para o funcionamento dos outros componentes do sistema de controlo interno. O ambiente de controlo não previne, nem deteta e corrige diretamente distorções. Pode, no entanto, influenciar a eficácia dos controlos nos outros componentes do sistema de controlo interno. Do mesmo modo, o processo de avaliação de risco da entidade e o seu processo de monitorização do sistema de controlo interno destinam-se a funcionar de forma a apoiar também todo o sistema de controlo interno.

A98. Uma vez que estes componentes são fundamentais para o sistema de controlo interno da entidade, quaisquer deficiências no seu funcionamento podem ter efeitos profundos na preparação das demonstrações financeiras. Consequentemente, a compreensão e avaliação destes componentes por parte do auditor afeta a identificação e a avaliação do auditor dos riscos de distorção material ao nível das demonstrações financeiras, e também pode afetar a identificação e a avaliação dos riscos de distorção material ao nível da asserção. Os riscos de distorção material ao nível da demonstração financeira afetam a conceção por parte do auditor de respostas globais, incluindo, tal como explicado na ISA 330, uma influência sobre a natureza, oportunidade e extensão dos procedimentos adicionais do auditor.[35]

Obtenção de uma compreensão do ambiente de controlo (Ref: Parágrafo 21)

Escalabilidade

A99. A natureza do ambiente de controlo numa entidade menos complexa é suscetível de ser diferente do ambiente de controlo numa entidade mais complexa. Por exemplo, os encarregados da governação em entidades menos complexas podem não incluir um membro independente ou externo, e o papel de governação pode ser assumido diretamente pelo proprietário-gestor quando não houver outros proprietários. Assim, algumas considerações sobre o ambiente de controlo da entidade podem ser menos relevantes ou podem não ser aplicáveis.

A100. Além disso a prova de auditoria sobre elementos do ambiente de controlo em entidades menos complexas pode não estar disponível em forma documental, nomeadamente quando a comunicação entre o órgão de gestão e outros funcionários for informal, mas a prova pode ainda assim ser adequadamente relevante e fiável nas circunstâncias.

[35] ISA 330, parágrafos A1-A3

Exemplos:

- A estrutura organizacional numa entidade menos complexa será provavelmente mais simples e poderá incluir um pequeno número de colaboradores envolvidos em funções relacionadas com o relato financeiro.
- Se o papel da governação for assumido diretamente pelo proprietário-gestor, o auditor pode determinar que a independência dos responsáveis pela governação não é relevante.
- Entidades menos complexas podem não ter um código de conduta escrito, mas, em vez disso, desenvolver uma cultura que enfatize a importância da integridade e do comportamento ético através da comunicação oral e pelo exemplo do órgão de gestão. Consequentemente, as atitudes, a sensibilização e as ações do órgão de gestão ou do proprietário-gestor são particularmente importantes para a compreensão do auditor sobre o ambiente de controlo de uma entidade menos complexa.

Compreensão do ambiente de controlo (Ref: Parágrafo21 (a))

A101. A prova de auditoria para a compreensão do ambiente de controlo por parte do auditor pode ser obtida através de uma combinação de indagações e outros procedimentos de avaliação de risco (isto é, corroborar indagações através da observação ou inspeção dos documentos).

A102. Ao considerar até que ponto o órgão de gestão demonstra um compromisso com a integridade e os valores éticos, o auditor pode obter um entendimento através de indagações ao órgão de gestão e colaboradores, e através da análise de informações de fontes externas, sobre:

- Como o órgão de gestão comunica aos colaboradores as suas opiniões sobre práticas comerciais e comportamento ético;
- Inspecionando o código de conduta escrito do órgão de gestão e observando se o órgão de gestão age de forma a apoiar esse código.

Avaliação do ambiente de controlo (Ref: Parágrafo 21(b))

Por que razão o auditor avalia o ambiente de controlo

A103. A avaliação do auditor da forma como a entidade demonstra comportamento consistente com o compromisso da entidade com a integridade e os valores éticos; se o ambiente de controlo proporciona uma base adequada para os outros componentes do sistema de controlo interno da entidade; e se quaisquer deficiências de controlo identificadas comprometem os outros componentes do sistema de controlo interno, ajuda o auditor na identificação de potenciais problemas nos outros componentes do sistema de controlo interno. Isto porque o ambiente de controlo é fundamental para os outros componentes do sistema de controlo interno da entidade. Esta avaliação também pode ajudar o auditor a compreender os riscos enfrentados pela entidade e, consequentemente, a identificar e avaliar os riscos de distorção material ao nível da demonstração financeira e da asserção (ver parágrafo A86).

Avaliação do auditor sobre o ambiente de controlo

A104. A avaliação do ambiente de controlo por parte do auditor baseia-se no entendimento obtido em conformidade com o parágrafo 21(a).

A105. Algumas entidades podem ser dominadas por um único indivíduo que pode atuar com uma grande margem de manobra. As ações e atitudes desse indivíduo podem ter um efeito profundo na cultura da entidade, o que, por sua vez, pode ter um efeito profundo no ambiente de controlo. Tal efeito pode ser positivo ou negativo.

Exemplo:

O envolvimento direto de um único indivíduo pode ser fundamental para permitir que a entidade atinja os seus objetivos de crescimento e outros, e pode também contribuir significativamente para um sistema eficaz de controlo interno. Por outro lado, essa concentração de conhecimento e autoridade também pode conduzir a uma maior suscetibilidade a distorção devido a substituição de controlos pelo órgão de gestão.

A106. O auditor pode considerar como os diferentes elementos do ambiente de controlo podem ser influenciados pela filosofia e pelo estilo de funcionamento da gestão de topo, tendo em conta o envolvimento de membros independentes dos encarregados da governação.

A107. Embora o ambiente de controlo possa constituir uma base adequada para o sistema de controlo interno e possa ajudar a reduzir o risco de fraude, um ambiente de controlo adequado não é necessariamente um fator eficaz de dissuasão da fraude.

> **Exemplo**:
>
> As políticas e procedimentos de recursos humanos direcionados para a contratação de pessoal competente para as áreas financeira, contabilística e de TI podem atenuar o risco de erros no processamento e registo de informações financeira. No entanto, tais políticas e procedimentos não conseguem atenuar a substituição de controlos pela gestão de topo (por exemplo, para sobrestimar resultados).

A108. A avaliação do auditor sobre o ambiente de controlo no que diz respeito à utilização das TI por parte da entidade, pode incluir matérias como:

- Se a governação sobre as TI é proporcional à natureza e complexidade da entidade e às suas operações comerciais possibilitadas por TI, incluindo a complexidade ou maturidade da plataforma ou arquitetura tecnológica da entidade e até que ponto a entidade depende de aplicações de TI para apoiar o seu relato financeiro.
- A estrutura organizacional de gestão em matéria de TI e os recursos atribuídos (por exemplo, se a entidade investiu num ambiente informático adequado e nos melhoramentos necessários, ou se foi utilizado um número suficiente de indivíduos devidamente qualificados, incluindo quando a entidade utiliza *software* comercial (sem alterações ou com modificações limitadas)).

Obtenção de um entendimento do processo de avaliação de risco da entidade (Ref: Parágrafo 22-23)

Compreensão do processo de avaliação de riscos da entidade (Ref: Parágrafo 22 (a))

A109. Tal como explicado no parágrafo A62, nem todos os riscos de negócio dão origem a riscos de distorção material. Ao compreender como o órgão de gestão e os encarregados da governação identificaram os riscos de negócio relevantes para a preparação das demonstrações financeiras, e decidiram sobre as ações para fazer face a esses riscos, as matérias que o auditor pode considerar incluem a forma como o órgão de gestão ou, se for caso disso, os encarregados da governação:

- Especificou os objetivos da entidade com rigor e clareza suficientes para permitir a identificação e avaliação dos riscos relacionados com os objetivos;
- Identificou os riscos para atingir os objetivos da entidade e analisou os riscos como base para determinar como os riscos devem ser geridos; e
- Considerou o potencial de fraude ao considerar os riscos para atingir os objetivos da entidade.[36]

A110. O auditor pode considerar as implicações desses riscos de negócio para a preparação das demonstrações financeiras da entidade e para outros aspetos do seu sistema de controlo interno.

Avaliação do processo de avaliação dos riscos da entidade (Ref: Parágrafo 22(b))

Por que razão o auditor avalia se o processo de avaliação de risco da entidade é adequado

A111. A avaliação do auditor do processo de avaliação de risco da entidade pode ajudar o auditor a compreender onde a entidade identificou riscos que podem ocorrer e como a entidade respondeu a esses riscos. A avaliação do auditor sobre a forma como a entidade identifica os seus riscos de negócio e a forma como avalia e aborda esses riscos ajuda o auditor a compreender se os riscos enfrentados pela entidade foram identificados, avaliados e abordados conforme adequado à natureza e complexidade da entidade. Esta avaliação também pode ajudar o auditor a identificar e avaliar riscos de distorção material aos níveis da demonstração financeira e da asserção (ver parágrafo A86).

Avaliar se o processo de avaliação de risco da entidade é adequado (Ref: Parágrafo 22(b))

A112. A avaliação do auditor sobre a adequação do processo de avaliação dos riscos da entidade baseia-se no entendimento obtido em conformidade com o parágrafo 22(a).

Escalabilidade

A113. Se o processo de avaliação de risco da entidade é adequado às circunstâncias da entidade, considerando a

[36] ISA 240, parágrafo 19

natureza e complexidade da entidade, é uma questão de julgamento profissional do auditor.

> **Exemplo**:
>
> Em algumas entidades menos complexas, e em particular nas entidades geridas pelos proprietários, pode ser efetuada uma avaliação adequada dos riscos através do envolvimento direto do órgão de gestão ou do proprietário-gestor (por exemplo, o órgão de gestão ou o proprietário-gestor pode dedicar rotineiramente tempo ao acompanhamento das atividades dos concorrentes e de outros desenvolvimentos no mercado para identificar riscos de negócios emergentes). A prova desta avaliação de risco neste tipo de entidades muitas vezes não está formalmente documentada, mas pode ser evidente pelas discussões que o auditor tem com o órgão de gestão de que o órgão de gestão está, de facto, a executar procedimentos de avaliação de riscos.

Obtenção da compreensão do processo da entidade para monitorizar o sistema de controlo interno da entidade (Ref: Parágrafo 24)

Escalabilidade

A114. Em entidades menos complexas, e em particular nas entidades geridas por proprietários, o conhecimento do auditor sobre o processo de monitorização do sistema de controlo interno centra-se frequentemente na forma como o órgão de gestão ou o proprietário-gestor está diretamente envolvido nas operações, uma vez que pode não existir qualquer outra atividade de monitorização.

> **Exemplo**:
>
> O órgão de gestão pode receber reclamações de clientes sobre incorreções nos extratos mensais que m o proprietário-gestor para problemas com o momento em que os pagamentos dos clientes estão a ser reconhecidos nos registos contabilísticos.

A115. Para as entidades em que não exista um processo formal de monitorização do sistema de controlo interno, a compreensão do processo de monitorização do sistema de controlo interno pode incluir a compreensão das revisões periódicas de informação contabilística de gestão que são concebidas para contribuir para a forma como a entidade previne ou deteta distorções.

Compreender o processo da entidade para monitorizar o sistema de controlo interno (Ref: Parágrafo 24(a))

A116. As matérias que podem ser relevantes para o auditor considerar quando entender como a entidade monitoriza o seu sistema de controlo interno incluem:

- A conceção das atividades de monitorização, por exemplo, em que medida se trata de monitorização periódica ou contínua;
- O desempenho e frequência das atividades de monitorização;
- A avaliação dos resultados das atividades de monitorização, em tempo oportuno, para determinar se os controlos foram eficazes; e
- Como as deficiências identificadas têm sido abordadas através de ações corretivas adequadas, incluindo a comunicação oportuna de tais deficiências aos responsáveis pela tomada de medidas corretivas.

A117. O auditor também pode analisar a forma como o processo da entidade para monitorizar o sistema de controlo interno aborda a monitorização dos controlos de processamento de informação que envolvem a utilização de TI. Isto pode incluir, por exemplo:

- Controlos para monitorizar ambientes complexos de TI que:
  - Avaliem a eficácia contínua dos controlos de processamento de informação e os modifiquem, se for caso disso, quando haja alterações nas condições; ou
  - Avaliem a eficácia operacional dos controlos de processamento de informação.
- Controlos que monitorizam as permissões aplicadas em controlos de processamento automatizado de informação que impõem a segregação de funções.
- Controlos que monitorizam a forma como os erros ou deficiências de controlo relacionados com a automatização do relato financeiro são identificados e tratados.

Compreender a função de auditoria interna da entidade (Ref: Parágrafo 24(a)ii)

O apêndice 4 apresenta considerações adicionais para a compreensão da função de auditoria interna da entidade.

A118. As indagações do auditor a indivíduos adequados no âmbito da função de auditoria interna ajudam o auditor a compreender a natureza das responsabilidades da função de auditoria interna. Se o auditor determinar que as responsabilidades da função estão relacionadas com o relato financeiro da entidade, o auditor poderá obter uma compreensão mais aprofundada das atividades executadas ou a serem executadas, pela da função de auditoria interna, revendo o plano de auditoria da função de auditoria interna para o período, caso exista, e discutir esse plano com as pessoas adequadas dentro da função. Este entendimento, juntamente com as informações obtidas nas indagações feitas pelo auditor, também pode proporcionar informações diretamente relevantes para a identificação e avaliação por parte do auditor, dos riscos de distorção material. Se, com base no entendimento preliminar do auditor sobre a função de auditoria interna, o auditor espera utilizar o trabalho da função de auditoria interna para modificar a natureza ou a oportunidade, ou reduzir a extensão dos procedimentos de auditoria a executar, aplica-se a ISA 610 (Revista 2013)[37] .

Outras fontes de informação usadas no processo da entidade para monitorizar o sistema de controlo interno

Compreensão das fontes de informação (Ref: Parágrafo 24(b))

A119. As atividades de monitorização do órgão de gestão podem utilizar informações em comunicações de partes externas, tais como reclamações de clientes ou comentários do regulador que possam indicar problemas ou realçar áreas que precisam de ser melhoradas.

Por que razão se exige que o auditor compreenda as fontes de informação usadas para a monitorização do sistema de controlo interno da entidade

A120. A compreensão do auditor sobre as fontes de informação usadas pela entidade para monitorização do sistema de controlo interno da entidade, incluindo se as informações usadas são relevantes e fiáveis, ajuda o auditor a avaliar se o processo da entidade para monitorizar o sistema de controlo interno da entidade é adequado. Se o órgão de gestão assume que as informações usadas para o controlo são relevantes e fiáveis sem ter uma base para esse pressuposto, os erros que possam existir na informação podem potencialmente levar o órgão de gestão a tirar conclusões incorretas das suas atividades de monitorização.

Avaliação do processo da entidade para monitorizar o sistema de controlo interno Ref: Para 24(c))

Por que razão o auditor avalia se o processo da entidade para monitorizar o sistema de controlo interno é adequado

A121. A avaliação do auditor sobre a forma como a entidade realiza avaliações contínuas e separadas para monitorizar a eficácia dos controlos ajuda o auditor a compreender se os outros componentes do sistema de controlo interno da entidade estão presentes e em funcionamento, ajudando assim a compreender os outros componentes do sistema de controlo interno da entidade. Esta avaliação também pode ajudar o auditor a identificar e avaliar o risco de distorção materiais aos níveis da demonstração financeira e da asserção (ver parágrafo A86).

Avaliar se o processo da entidade para monitorizar o sistema de controlo interno é adequado (Ref: Parágrafo 24(c))

A122. A avaliação do auditor sobre a adequação do processo da entidade para monitorizar o sistema de controlo interno baseia-se na compreensão do auditor sobre o processo da entidade para monitorizar o sistema de controlo interno.

Sistema de Informação e Atividades de Comunicação e Controlo (Ref: Parágrafo 25-26)

A123. Os controlos no sistema de informação e na comunicação e nos componentes das atividades de controlo são principalmente controlos diretos (isto é, controlos suficientemente precisos para prevenir, detetar ou corrigir distorções ao nível da asserção).

Por que razão se exige que o auditor compreenda o sistema de informação e a comunicação e os controlos na componente das atividades de controlo

A124. Exige-se que o auditor compreenda o sistema de informação e comunicação da entidade porque compreender as políticas da entidade que definem os fluxos de transações e outros aspetos das atividades de processamento de informação da entidade relevantes para a preparação das demonstrações financeiras, e avaliar se a componente apoia adequadamente a preparação das demonstrações financeiras da entidade, apoia a identificação e avaliação por parte do auditor dos riscos de distorção material ao nível da asserção. Este

[37] ISA 610 (Revisto em 2013), *Utilização do Trabalho de Auditores Internos*

entendimento e avaliação também podem resultar na identificação de riscos de distorção material ao nível da demonstração financeira quando os resultados dos procedimentos do auditor forem incompatíveis com as expectativas acerca do sistema de controlo interno da entidade que possam ter sido definidas com base nas informações obtidas durante o processo de aceitação ou continuação do trabalho (ver parágrafo A86).

A125. Exige-se que o auditor identifique controlos específicos na componente das atividades de controlo, avalie a conceção e determine se os controlos foram implementados, uma vez que ajuda a compreensão por parte do auditor da abordagem do órgão de gestão para fazer face a determinados riscos e, consequentemente, proporciona uma base para a conceção e execução de procedimentos de auditoria adicionais que respondam a esses riscos, conforme exigido pela ISA 330. Quanto mais elevado no espectro de risco inerente um risco for avaliado, mais persuasiva necessita ser a prova de auditoria. Mesmo quando o auditor não planeia testar a eficácia operacional dos controlos identificados, o conhecimento do auditor pode ainda assim afetar a conceção, a oportunidade e a extensão dos procedimentos de auditoria substantivos que respondam aos riscos relacionados de distorção material.

A natureza iterativa da compreensão e avaliação do auditor do sistema de informação e comunicação, e as atividades de controlo

A126. Tal como explicado no parágrafo A49, a compreensão do auditor sobre a entidade e o seu ambiente, bem como o referencial de relatos financeiro aplicável, pode ajudar o auditor a desenvolver expectativas iniciais sobre as classes de transações, saldos de contas e divulgações que possam ser categorias significativas de transações, saldos de contas e divulgações. Ao obter uma compreensão do sistema de informação e da componente de comunicação em conformidade com o parágrafo 25 (a), o auditor pode utilizar estas expectativas iniciais para determinar a extensão da compreensão que é necessária obter sobre as atividades de processamento de informação da entidade.

A127. A compreensão do auditor sobre o sistema de informação inclui a compreensão das políticas que definem fluxos de informação relativos às classes de transações, saldos de contas e divulgações significativas da entidade, bem como outros aspetos relacionados com as atividades de processamento de informação da entidade. Estas informações, bem como as informações obtidas a partir da avaliação do sistema de informação pelo auditor podem confirmar ou influenciar ainda mais as expectativas do auditor acerca das classes de transações, saldos de contas e divulgações significativas inicialmente identificadas (ver parágrafo A126).

A128. Ao obter uma compreensão de como as informações relativas a classes de transações, saldos de contas e divulgações significativas fluem para, através de e para fora do sistema de informação da entidade, o auditor também pode identificar controlos na componente das atividades de controlo que devem ser identificados em conformidade com o parágrafo 26(a). A identificação e avaliação dos controlos por parte do auditor na componente das atividades de controlo pode, em primeiro lugar, centrar-se nos controlos sobre os lançamentos contabilísticos e nos controlos em que o auditor planeia testar a respetiva eficácia operacional ao conceber a natureza, oportunidade e extensão dos procedimentos substantivos.

A129. A avaliação do auditor sobre o risco inerente também pode influenciar a identificação de controlos na componente das atividades de controlo. Por exemplo, a identificação do auditor de controlos relativos a riscos significativos pode só ser identificável quando o auditor já tiver avaliado o risco inerente ao nível da asserção em conformidade com o parágrafo 31. Além disso, os controlos que abordam os riscos para os quais o auditor determinou que, por si só, os procedimentos substantivos não proporcionam prova de auditoria suficiente (em conformidade com o parágrafo 33) podem também só ser identificáveis após o auditor efetuar as avaliações de risco inerente.

A130. A identificação e avaliação do auditor sobre os riscos de distorção material ao nível da asserção é influenciada pelas duas atividades seguintes do auditor:

- Compreensão das políticas da entidade para as suas atividades de processamento de informação no sistema de informação e na componente de comunicação, e
- Identificação e avaliação dos controlos na componente das atividades de controlo.

Obtenção de uma compreensão do sistema de informação e comunicação (Ref: Parágrafo 25)

O apêndice 3, parágrafos 15-19, apresenta considerações adicionais relativas ao sistema de informação e à comunicação.

Escalabilidade

A131. O sistema de informação, e os processos de negócio relacionados, em entidades menos complexas são suscetíveis de ser menos sofisticados do que em entidades maiores, e são suscetíveis de envolver um ambiente de TI menos complexo; no entanto, a função do sistema de informação é igualmente importante. Entidades menos complexas com envolvimento direto do órgão de gestão podem não necessitar de descrições extensivas de procedimentos contabilísticos, registos contabilísticos sofisticados ou políticas escritas. A compreensão dos aspetos relevantes do sistema de informação da entidade pode, consequentemente, exigir menos esforço numa auditoria de uma entidade menos complexa, podendo implicar uma maior quantidade de indagação do que observação ou inspeção de documentação. No entanto, a necessidade de obter um entendimento continua a ser importante para proporcionar uma base para a conceção de novos procedimentos de auditoria em conformidade com a ISA 330 e pode ajudar ainda mais o auditor a identificar ou avaliar os riscos de distorção material (ver parágrafo A86).

Obtenção de uma compreensão do sistema de informação (Ref: Parágrafo 25 (a))

A132. Incluídos no sistema de controlo interno da entidade estão aspetos relacionados com os objetivos de relato da entidade, incluindo os seus objetivos de relato financeiro, mas também podem incluir aspetos relacionados com as suas operações ou objetivos de conformidade, quando tais aspetos são relevantes para o relato financeiro. Compreender a forma como a entidade inicia as transações e capta informações, como parte da compreensão por parte do auditor sobre o sistema de informação, pode incluir informações sobre os sistemas da entidade (as suas políticas) concebidas para abordarem objetivos de conformidade e operacionais, uma vez que tais informações são relevantes para a preparação das demonstrações financeiras. Além disso, algumas entidades podem ter sistemas de informação altamente integrados de forma que os controlos possam ser concebidos de maneira a alcançar simultaneamente objetivos de relato financeiro, objetivos de conformidade e operacionais, e combinações dos mesmos.

A133. A compreensão do sistema de informação da entidade inclui também uma compreensão dos recursos a utilizar nas atividades de processamento de informação da entidade. As informações sobre os recursos humanos envolvidos que podem ser relevantes para a compreensão dos riscos relativos à integridade do sistema de informação incluem:

- A competência das pessoas que realizam o trabalho;
- Se existem recursos adequados; e
- Se existe uma adequada segregação de funções.

A134. As matérias que o auditor pode considerar quando compreender as políticas que definem os fluxos de informação relativas às classes de transações, saldos de contas e divulgações significativas do sistema de informação e componente de comunicação incluem a natureza:

(a) Dos dados ou informações relativas a transações, outros acontecimentos e condições que serão processados;

(b) Do processamento da informação para manter a integridade desses dados ou informações; e

(c) Dos processos de informação, pessoal e outros recursos utilizados no processo de processamento de informação.

A135. A obtenção de um conhecimento dos processos negócio da entidade, que inclui a forma como as transações são originadas, ajuda o auditor a obter um entendimento do sistema de informação da entidade de forma adequada às circunstâncias da entidade.

A136. A compreensão do auditor sobre o sistema de informação pode ser obtida de várias formas e pode incluir:

- Indagações ao pessoal relevante sobre os procedimentos utilizados para iniciar, registar, processar e reportar transações ou sobre o processo de relato financeiro da entidade;
- Inspeção de manuais de política ou de processo ou outra documentação do sistema de informação da entidade;
- Observação do cumprimento das políticas ou procedimentos por parte do pessoal da entidade, ou
- Selecionar transações e rastreá-las através do processo aplicável no sistema de informação (ou seja, executar análises de funcionamento (*walk-through)).*

Ferramentas e técnicas automatizadas

A137. O auditor também pode utilizar técnicas automatizadas para obter acesso direto a, ou fazer um *download* digital a partir de bases de dados do sistema de informação da entidade que armazenam registos contabilísticos de transações. Ao aplicar ferramentas ou técnicas automatizadas a estas informações, o auditor pode confirmar o entendimento obtido sobre a forma como as transações fluem através do sistema de informação fazendo o rastreio dos lançamentos de diário, ou outros registos digitais relacionados com uma determinada transação, ou toda uma população de transações, desde o início nos registos contabilísticos até ao registo no livro-razão geral. A análise do da totalidade ou conjuntos grandes de transações também pode resultar na identificação de variações em relação aos procedimentos de processamento normais ou esperados para estas transações, o que pode resultar na identificação de riscos de distorção material.

Informações obtidas fora dos livros razão-geral e subsidiários

A138. As demonstrações financeiras podem conter informações obtidas fora dos livros razão-geral e subsidiários. Exemplos dessas informações que o auditor pode considerar incluem:

- Informação obtida a partir de contratos de locação relevantes para divulgações nas demonstrações financeiras.
- Informação divulgada nas demonstrações financeiras que seja produzida pelo sistema de gestão de risco de uma entidade.
- Informação de justo valor produzida por peritos do órgão de gestão e divulgada nas demonstrações financeiras.
- Informações divulgadas nas demonstrações financeiras obtidas a partir de modelos, ou de outros cálculos utilizados para desenvolver estimativas contabilísticas reconhecidas ou divulgadas nas demonstrações financeiras, incluindo informações relativas aos dados e pressupostos subjacentes utilizados nesses modelos, tais como:
  - Pressupostos desenvolvidos internamente que podem afetar a vida útil de um ativo; ou
  - Informações, como taxas de juro que são afetadas por fatores fora do controlo da entidade.
- Informação divulgada nas demonstrações financeiras sobre análises de sensibilidade derivadas de modelos financeiros que demonstram que o órgão de gestão considerou pressupostos alternativos.
- Informação reconhecida ou divulgada nas demonstrações financeiras obtidas a partir das declarações e registos fiscais de uma entidade.
- Informações divulgadas nas demonstrações financeiras obtidas a partir de análises preparadas para apoiar a avaliação por parte do órgão de gestão da capacidade da entidade de conseguir continuar a operar numa ótica de continuidade, tais como divulgações, se houver, relacionadas com acontecimentos ou condições que tenham sido identificadas que possam levantar dúvidas significativas sobre a capacidade da entidade para continuar a operar numa ótica de continuidade.[38]

A139. Certas quantias ou divulgações nas demonstrações financeiras da entidade (tais como divulgações sobre risco de crédito, risco de liquidez e risco de negócio) podem basear-se em informações obtidas do sistema de gestão de risco da entidade. No entanto, não se exige que o auditor compreenda todos os aspetos do sistema de gestão de riscos, mas sim que utilize o julgamento profissional para determinar a compreensão necessária.

A utilização, por parte da entidade, das tecnologias da informação no sistema de informação

Por que razão o auditor compreende o ambiente de TI relevante para o sistema de informação

A140. A compreensão do auditor sobre o sistema de informação inclui o ambiente de TI relevante para os fluxos de transações e o processamento de informações no sistema de informação da entidade, uma vez que a utilização, por parte da entidade, de aplicações informáticas ou outros aspetos no ambiente de TI pode dar origem a riscos decorrentes da utilização de TI.

A141. A compreensão do modelo de negócio da entidade e a forma como integra a utilização de TI também podem proporcionar um contexto útil à natureza e extensão das TI esperadas no sistema de informação.

Compreender a utilização de TI por parte da entidade

[38] ISA 570 (Revista), parágrafos 19-20

A142. A compreensão por parte do auditor sobre o ambiente de TI pode centrar-se na identificação e compreensão da natureza e do número de aplicações específicas de TI e outros aspetos do ambiente de TI relevantes para os fluxos de transações e processamento de informação no sistema de informação. Alterações no fluxo de transações ou informação dentro do sistema de informação podem resultar de alterações aos programas das aplicações de TI, ou alterações diretas aos dados nas bases de dados envolvidas no processamento, ou armazenamento dessas transações ou informações.

A143. O auditor pode identificar as aplicações de TI e a infraestrutura de TI que as suporta, simultaneamente com a compreensão por parte do auditor sobre a forma como as informações relativas a classes de transações, saldos de contas e divulgações significativas fluem para, através de e para fora do sistema de informação da entidade.

Obtenção de um entendimento da comunicação da entidade (Ref: Parágrafo 25(b))

Escalabilidade

A144. Em entidades maiores e mais complexas, a informação que o auditor pode considerar ao obter a compreensão sobre a comunicação da entidade pode vir de manuais de política e manuais de relato financeiro.

A145. Em entidades menos complexas, a comunicação pode ser menos estruturada (por exemplo, os manuais formais podem não ser utilizados) devido a menos níveis de responsabilidade e maior visibilidade e disponibilidade por parte do órgão de gestão. Independentemente da dimensão da entidade, canais de comunicação abertos facilitam o relato de exceções e a atuação sobre estas.

Avaliar se os aspetos relevantes do sistema de informação apoiam a preparação das demonstrações financeiras da entidade (Ref: Parágrafo 25(c))

A146. A avaliação do auditor sobre se o sistema de informação e a comunicação da entidade apoiam adequadamente a preparação das demonstrações financeiras baseia-se no entendimento obtido no parágrafo 25(a) –(b).

Atividades de controlo (Ref: Parágrafo 26)

Controlos na componente das atividades de controlo

O apêndice 3, parágrafos 20 e 21, estabelece considerações adicionais relativas às atividades de controlo.

A147. A componente das atividades de controlo inclui controlos concebidos para assegurar a adequada aplicação de políticas (que também são controlos) em todos os outros componentes do sistema de controlo interno da entidade, e inclui controlos diretos e indiretos.

Exemplo:

Os controlos que uma entidade estabeleceu para garantir que o seu pessoal está a contar e a registar adequadamente o inventário físico anual relacionam-se diretamente com os riscos de distorção material relevantes para as asserções de existência e plenitude do saldo da conta de inventários.

A148. A identificação e avaliação dos controlos, por parte do auditor, na componente das atividades de controlo centra-se nos controlos de processamento de informação, que são controlos aplicados durante o processamento de informação no sistema de informação da entidade que abordam diretamente os riscos para a integridade da informação (ou seja, a plenitude, rigor e validade das transações e outras informações). No entanto, não se exige que o auditor identifique e avalie todos os controlos de processamento de informação relacionados com as políticas da entidade que definem os fluxos de transações e outros aspetos das atividades de processamento de informação da entidade para as classes de transações, saldos de contas e divulgações significativas.

A149. Também podem existir controlos diretos no ambiente de controlo, no processo de avaliação dos riscos da entidade ou no processo da entidade para monitorizar o sistema de controlo interno, que podem ser identificados em conformidade com o parágrafo 26. No entanto, quanto mais indireta for a relação entre os controlos que suportam outros controlos e o controlo que está a ser considerado, menos eficaz poderá ser o controlo na prevenção, ou na deteção e correção das distorções relacionadas.

Exemplo:

Normalmente, a revisão por um gestor de vendas de um resumo da atividade de vendas de lojas específicas por região está apenas indiretamente relacionada com os riscos de distorção material relevantes para a asserção de plenitude do rédito de vendas. Consequentemente, pode ser menos eficaz na redução do risco para essa

asserção do que os controlos mais diretamente relacionados, como a conferência dos documentos de expedição com os documentos de faturação.

A150. O parágrafo 26 também exige que o auditor identifique e avalie os controlos gerais de TI para aplicações informáticas e outros aspetos do ambiente de TI que o auditor determinou estarem sujeito a riscos decorrentes da utilização de TI, uma vez que os controlos gerais de TI suportam o funcionamento eficaz continuado dos controlos de processamento de informação. Um controlo geral de TI por si só normalmente não é suficiente para fazer face a um risco de distorção material ao nível da asserção.

A151. Os controlos em que se exige que o auditor identifique e avalie a conceção, e determine a implementação, em conformidade com o parágrafo 26, são:

- Controlos em que o auditor planeia testar a eficácia operacional para determinar a natureza, oportunidade e extensão dos procedimentos substantivos. A avaliação destes controlos constitui a base para a conceção, por parte do auditor, dos procedimentos para testar os controlos, em conformidade com a ISA 330. Estes controlos também incluem controlos que abordam riscos para os quais os procedimentos substantivos por si só não proporcionam prova de auditoria suficiente.
- Controlos que incluem controlos que abordam riscos e controlos significativos sobre os lançamentos no diário. A identificação e avaliação desses controlos por parte do auditor também pode influenciar a compreensão do auditor sobre os riscos de distorção material, incluindo a identificação de riscos adicionais de distorção material (ver parágrafo A95). Este entendimento também proporciona a base para a conceção, por parte do auditor, da natureza, oportunidade e extensão dos procedimentos de auditoria substantivos que respondam aos riscos de distorção material relacionados que foram avaliados.
- Outros controlos que o auditor considera adequados para permitir cumprir os objetivos do parágrafo 13 no que diz respeito aos riscos ao nível da asserção, com base no julgamento profissional do auditor.

A152. Exige-se que os controlos na componente das atividades de controlo sejam identificados quando esses controlos satisfaçam um ou mais dos critérios incluídos no parágrafo 26(a). No entanto, quando existem múltiplos controlos em que cada um alcança o mesmo objetivo, é desnecessário identificar cada um dos controlos relacionados com esse objetivo.

Tipos de controlos na componente das atividades de controlo (Ref: Parágrafo 26)

A153. Exemplos de controlos na componente das atividades de controlo incluem autorizações e aprovações, reconciliações, verificações (tais como verificações de edição e validação ou cálculos automatizados), segregação de funções e controlos físicos ou lógicos, incluindo os que abordam a salvaguarda dos ativos.

A154. Os controlos na componente das atividades de controlo também podem incluir controlos estabelecidos pelo órgão de gestão que abordam os riscos de distorção material relacionados com as divulgações não preparadas de acordo com o referencial de informação financeira aplicável. Esses controlos podem relacionar-se com informações incluídas nas demonstrações financeiras obtidas fora dos livros de razão geral e subsidiários.

A155. Independentemente de os controlos estarem dentro do ambiente de TI ou dos sistemas manuais, os controlos podem ter vários objetivos e podem ser aplicados a vários níveis organizacionais e funcionais.

Escalabilidade (Ref: Parágrafo 26)

A156. Os controlos na componente das atividades de controlo para entidades menos complexas são suscetíveis de ser semelhantes aos dos das entidades maiores, mas a formalidade com que operam pode variar. Além disso, em entidades menos complexas, mais controlos podem ser diretamente executados pelo órgão de gestão.

Exemplo:

A autoridade exclusiva do órgão de gestão para a concessão de crédito a clientes e aprovação de compras significativas pode proporcionar um forte controlo sobre saldos e transações importantes da conta.

A157. Pode ser menos praticável estabelecer uma segregação de funções em entidades menos complexas que tenham menos trabalhadores. No entanto, numa entidade gerida pelo proprietário, o proprietário-gestor pode exercer uma supervisão mais eficaz através de um envolvimento direto do que numa entidade maior, o que pode compensar as oportunidades geralmente mais limitadas de segregação de funções. Embora, como também explicado na ISA 240, o controlo do órgão de gestão por um único indivíduo possa ser uma potencial deficiência

de controlo, uma vez que existe uma oportunidade de derrogação do controlo interno pelo órgão de gestão.[39]

Controlos que abordam os riscos de distorção material ao nível da asserção (Ref: Parágrafo 26(a))

Controlos que abordam riscos que são considerados um risco significativo (Ref: Parágrafo 26(a)(i))

A158. Independentemente de o auditor planear testar a eficácia operacional dos controlos que abordam riscos significativos, o entendimento obtido sobre a abordagem do órgão de gestão para fazer face a esses riscos pode constituir uma base para a conceção e execução de procedimentos substantivos que respondam a riscos significativos, tal como exigido pela ISA 330. [40] Embora os riscos relacionados com matérias significativas não rotineiras ou de julgamento sejam frequentemente menos suscetíveis de serem sujeitos a controlos de rotina, o órgão de gestão pode ter outras respostas destinadas a lidar com esses riscos. Consequentemente, a compreensão do auditor sobre se a entidade concebeu e implementou controlos para riscos significativos decorrentes de matérias não rotineiras ou de julgamento pode incluir se e como o órgão de gestão responde aos riscos. Tais respostas podem incluir:

- Controlos, tais como uma revisão dos pressupostos por altos quadros ou peritos.
- Processos documentados para estimativas contabilísticas.
- Aprovação por parte dos encarregados da governação.

> **Exemplo**:
>
> Sempre que existam acontecimentos pontuais, como a receção de uma notificação relativa a um processo legal significativo, a apreciação da resposta da entidade pode incluir matérias como em que medida estes são entregues a peritos adequados (como o aconselhamento jurídico interno ou externo), se foi efetuada uma avaliação do efeito potencial e como se propõe que as circunstâncias sejam divulgadas nas demonstrações financeiras.

A159. A ISA 240[41] exige que o auditor compreenda os controlos relacionados com os riscos avaliados de distorção material devido a fraude (que são tratados como riscos significativos), e explica ainda que é importante que o auditor obtenha uma compreensão dos controlos que o órgão de gestão concebeu, implementou e manteve para prevenir e detetar fraudes.

Controlos sobre os lançamentos de diário (Ref: Parágrafo 26(a)(ii))

A160. Os controlos que abordam os riscos de distorção material ao nível de asserção que se espera que sejam identificados para todas as auditorias são controlos sobre lançamentos de diário, porque a forma como uma entidade incorpora informações do processamento de transações no livro razão-geral normalmente envolve a utilização de lançamentos de diário, sejam eles padrão ou não padrão, ou automatizadas ou manuais. A extensão em que os outros controlos são identificados pode variar em função da natureza da entidade e da abordagem planeada pelo auditor para novos procedimentos de auditoria.

> **Exemplo:**
>
> Numa auditoria a uma entidade menos complexa, o sistema de informação da entidade pode não ser complexo e o auditor pode pretender não confiar na eficácia operacional dos controlos. Além disso, o auditor pode não ter identificado quaisquer riscos significativos ou quaisquer outros riscos de distorção material para os quais seja necessário que o auditor avalie a conceção dos controlos e determine se foram implementados. Nessa auditoria, o auditor pode concluir que não existem controlos identificados a não ser os controlos da entidade sobre os lançamentos de diário.

Ferramentas e técnicas automatizadas

A161. Nos sistemas de livro-razão geral manuais, os lançamentos de diário não-padrão podem ser identificados através da inspeção dos livros, lançamentos e documentação de suporte. Quando são utilizados procedimentos automatizados para manter o livro-razão geral e preparar demonstrações financeiras, esses lançamentos podem existir só sob forma eletrónica e, portanto, podem ser mais facilmente identificados através da utilização de técnicas automatizadas.

---

[39] ISA 240, parágrafo A28
[40] ISA 330, parágrafo 21
[41] ISA 240, parágrafos 28 e A33

Exemplo:

Numa auditoria a uma entidade menos complexa, o auditor poderá ser capaz de extrair uma lista completa de todos os lançamentos de diário para uma simples folha de cálculo. Pode então ser possível ao auditor ordenar os lançamentos de diário através da aplicação de uma variedade de filtros, tais como a quantia da moeda, o nome de quem preparou ou de quem reviu, os lançamentos de diário que afetam apenas o balanço e a demonstração de resultados, ou ver a lista pela data em que os lançamentos de diário foram contabilizados no livro-razão geral, de forma a ajudar o auditor a conceber respostas aos riscos identificados relativos aos lançamentos de diário.

Controlos para os quais o auditor planeia testar a eficácia operacional (Ref: Parágrafo 26 a(iii))

A162. O auditor determina se existem riscos de distorção material ao nível da asserção quando não é possível obter prova de auditoria adequada e suficiente apenas através de procedimentos substantivos. Exige-se que o auditor, em conformidade com a ISA 330,[42] conceba e efetue testes aos controlos que abordem esses riscos de distorção material quando os procedimentos substantivos não proporcionam prova de auditoria adequada e suficiente ao nível da asserção. Como resultado, quando existem tais controlos que abordam estes riscos, exige-se que tais controlos sejam identificados e avaliados.

A163. Em outros casos, quando o auditor planeia ter em conta a eficácia operacional dos controlos na determinação da natureza, oportunidade e extensão dos procedimentos substantivos em conformidade com a ISA 330, também se exige que tais controlos sejam identificados, uma vez que a ISA 330[43] exige que o auditor conceba e execute testes a esses controlos.

Exemplos:

O auditor pode planear testar a eficácia operacional dos controlos:

- Sobre as classes de transações de rotina porque tais testes podem ser mais eficazes ou eficientes para grandes volumes de transações homogéneas.
- Sobre a plenitude e rigor das informações produzidas pela entidade (por exemplo, controlos sobre a preparação de relatórios gerados pelo sistema), para determinar a fiabilidade dessas informações, quando o auditor tenciona ter em conta a eficácia operacional desses controlos na conceção e execução de procedimentos de auditoria adicionais.
- No que diz respeito a operações e objetivos de conformidade quando eles se referem a dados que o auditor avalia ou utiliza na execução de procedimentos de auditoria.

A164. Os planos do auditor para testar a eficácia operacional dos controlos também podem ser influenciados pelos riscos identificados de distorção material ao nível da demonstração financeira. Por exemplo, se forem identificadas deficiências relacionadas com o ambiente de controlo, isso poderá afetar as expectativas globais do auditor quanto à eficácia operacional dos controlos diretos.

Outros controlos que o auditor considera adequados (Ref: Parágrafo 26 (a)(iv))

A165. Outros controlos que o auditor pode considerar ser adequado identificar, avaliar a conceção e concluir sobre a implementação, podem incluir:

- Controlos que abordam riscos avaliados como mais elevados no espectro de risco inerente, mas que não foram considerados como sendo um risco significativo;
- Controlos relacionados com a reconciliação de registos detalhados com o livro-razão geral; ou
- Controlos adicionais da entidade utilizadora, se for utilizada uma organização de serviços.[44]

[42] ISA 330, parágrafo 8 b
[43] ISA 330, n.º 8 a
[44] ISA 402, *Considerações de auditoria relativas a uma entidade que utilize uma Organização de Serviços*

Identificação de aplicações de TI e outros aspetos do ambiente de TI, riscos decorrentes da utilização de TI e controlos gerais de TI (Ref: Parágrafo 26(b)-(c))

O apêndice 5 inclui características exemplo de aplicações de TI e outros aspetos do ambiente de TI, e orientações relacionadas com essas características, que podem ser relevantes na identificação de aplicações de TI e de outros aspetos do ambiente de TI sujeitos a riscos decorrentes da utilização de TI.

Identificação de aplicações de TI e outros aspetos do ambiente de TI (Ref: Parágrafo 26(b))

Por que razão o auditor identifica os riscos decorrentes da utilização de TI e controlos gerais de TI relacionados com as aplicações de TI identificadas e outros aspetos do ambiente de TI

A166. Compreender os riscos decorrentes da utilização de TI e dos controlos gerais de TI implementados pela entidade para fazer face a esses riscos pode afetar:

- A decisão do auditor sobre se deve testar a eficácia operacional dos controlos para fazer face aos riscos de distorção material ao nível da asserção;

Exemplo:

Quando os controlos gerais de TI não estão concebidos de forma eficaz ou adequada para fazer face aos riscos decorrentes da utilização de TI (por exemplo, os controlos não previnem nem detetam alterações não autorizadas a programas nem acessos não autorizados a aplicações de TI), isso pode afetar a decisão do auditor de confiar em controlos automatizados dentro das aplicações de TI afetadas.

- Avaliação do risco de controlo pelo auditor ao nível da asserção;

Exemplo:

A eficácia operacional contínua de um controlo de processamento de informação pode depender de certos controlos gerais de TI que previnam ou detetem alterações não autorizadas ao programa no controlo de processamento de informação de TI (ou seja, controlos de alteração de programa sobre a aplicação de TI relacionada). Nestas circunstâncias, a eficácia operacional esperada (ou a sua falta) do controlo geral das TI pode afetar a avaliação do risco de controlo pelo auditor (por exemplo, o risco de controlo pode ser maior quando se prevê que esses controlos gerais de TI sejam ineficazes ou se o auditor não planeia testar os controlos gerais de TI).

- A estratégia do auditor para testar informações produzidas pela entidade que é produzida ou envolve informações provenientes das aplicações de TI da entidade;

Exemplo:

Quando as informações produzidas pela entidade a serem usadas como prova de auditoria são produzidas por aplicações de TI, o auditor pode decidir testar controlos sobre relatórios gerados pelo sistema, incluindo a identificação e teste dos controlos gerais de TI que abordam os riscos de alterações inadequadas ou não autorizadas do programa ou alterações diretas de dados nos relatórios.

- Avaliação do auditor sobre o risco inerente ao nível da asserção; ou

Exemplo:

Quando houver alterações significativas ou extensivas programadas a uma aplicação de TI para responder a requisitos de relato novos ou revistos do referencial de relato financeiro aplicável, isto pode ser um indicador da complexidade dos novos requisitos e do seu efeito nas demonstrações financeiras da entidade. Quando tal programação extensiva ou alterações de dados ocorrem, a aplicação de TI também é suscetível de estar sujeita a riscos decorrentes da utilização de TI.

- A conceção de procedimentos de auditoria adicionais.

Exemplo:

Se os controlos de processamento de informações dependerem dos controlos gerais de TI, o auditor pode decidir testar a eficácia de funcionamento dos controlos gerais de TI, o que exigirá então a conceção de testes aos controlos para esses controlos gerais de TI. Se, nas mesmas circunstâncias, o auditor decidir não testar a eficácia de funcionamento dos controlos gerais de TI, ou se se espera que os controlos gerais das TI sejam ineficazes, os riscos relacionados decorrentes da utilização das TI podem ter de ser abordados através da conceção de procedimentos substantivos. Todavia, os riscos decorrentes da utilização de TI podem não conseguir ser abordados quando esses riscos se referirem a riscos para os quais os procedimentos substantivos por si só não proporcionam prova de auditoria adequada e suficiente. Nestas circunstâncias, o auditor poderá ter de analisar as implicações para a opinião da auditoria.

Identificação de aplicações de TI sujeitas a riscos decorrentes da utilização de TI

A167. Nas aplicações de TI relevantes para o sistema de informação, compreender a natureza e a complexidade dos processos específicos de TI e os controlos gerais de TI que a entidade tem em vigor podem ajudar o auditor a determinar quais as aplicações de TI em que a entidade está a confiar para processar e manter com rigor a integridade da informação no sistema de informação da entidade. Tais aplicações de TI podem estar sujeitas a riscos decorrentes da utilização de TI.

A168. Identificar as aplicações de TI que estão sujeitas a riscos decorrentes da utilização de TI implica ter em conta os controlos identificados pelo auditor, uma vez que esses controlos podem implicar a utilização de TI ou confiar em TI. O auditor pode concentrar-se em saber se uma aplicação de TI inclui controlos automatizados em que o órgão de gestão está a confiar e que o auditor identificou, incluindo controlos que abordem riscos para os quais os procedimentos substantivos por si só não proporcionam prova de auditoria adequada e suficiente. O auditor também pode analisar a forma como as informações são armazenadas e processadas no sistema de informação relativas a classes de transações, saldos de contas e divulgações significativas e se o órgão de gestão está a confiar nos controlos gerais de TI para manter a integridade dessas informações.

A169. Os controlos identificados pelo auditor podem depender de relatórios gerados pelo sistema, caso em que as aplicações de TI que produzem esses relatórios podem estar sujeitas a riscos decorrentes da utilização de TI. Em outros casos, o auditor pode planear não confiar nos controlos dos relatórios gerados pelo sistema e planear testar diretamente as entradas e saídas desses relatórios, caso em que o auditor pode não identificar as aplicações de TI relacionadas como estando sujeitas a riscos decorrentes das TI.

Escalabilidade

A170. A extensão da compreensão do auditor sobre os processos de TI, incluindo em que medida a entidade dispõe de controlos gerais de TI, variará em função da natureza e das circunstâncias da entidade e do seu ambiente de TI, bem como com base na natureza e extensão dos controlos identificados pelo auditor. O número de aplicações de TI sujeitas a riscos decorrentes da utilização de TI também variará em função destes fatores.

Exemplos:

- É improvável que uma entidade que utilize software comercial e não tenha acesso ao código fonte para fazer quaisquer alterações nos programas tenha um processo para alterações de programas, mas pode ter um processo ou procedimentos para configurar o *software* (por exemplo, o plano de contas, parâmetros ou patamares de relato). Além disso, a entidade pode ter um processo ou procedimentos para gerir o acesso à aplicação (por exemplo, um determinado indivíduo com acesso administrativo ao *software* comercial). Nestas circunstâncias, é pouco provável que a entidade tenha ou necessite de controlos gerais de TI formalizados.
- Em contrapartida, uma entidade maior pode confiar em grande medida nas TI e o ambiente de TI pode envolver múltiplas aplicações de TI e os processos de TI para gerir o ambiente de TI podem ser complexos (por exemplo, existe um departamento de TI dedicado que desenvolve e implementa alterações de programas e gere os direitos de acesso), incluindo o facto de que a entidade implementou controlos gerais de TI formalizados sobre os seus processos de TI.
- Quando o órgão de gestão não está a confiar em controlos automatizados ou controlos gerais de TI para processar transações ou fazer a manutenção f de dados, e o auditor não identificou quaisquer controlos automatizados ou outros controlos de processamento de informação (nem qualquer outro que dependa de controlos gerais de TI), o auditor pode planear testar diretamente qualquer informação produzida pela entidade que envolva TI e pode não identificar quaisquer aplicações de TI sujeitas a riscos decorrentes da utilização de TI.

- Quando o órgão de gestão confia numa aplicação de TI para processar ou fazer a manutenção de dados e o volume de dados é significativo, e o órgão de gestão confia na aplicação de TI para executar controlos automatizados que o auditor também identificou, é provável que a aplicação de TI esteja sujeita a riscos decorrentes da utilização de TI.

A171. Quando uma entidade tem maior complexidade no seu ambiente de TI, identificar as aplicações de TI e outros aspetos do ambiente de TI, determinar os riscos relacionados decorrentes da utilização de TI, e identificar controlos gerais de TI é suscetível de exigir o envolvimento de membros da equipa com competências especializadas em TI. É provável que esse envolvimento seja essencial, e possa ter de ser extenso em ambientes complexos de TI.

Identificação de outros aspetos do ambiente de TI que estão sujeitos a riscos decorrentes da utilização de TI

A172. Os outros aspetos do ambiente de TI que podem estar sujeitos a riscos decorrentes da utilização de TI incluem a rede, o sistema operativo e as bases de dados e, em determinadas circunstâncias, as ligações entre aplicações de TI. Geralmente, outros aspetos do ambiente de TI não são identificados quando o auditor não identifica aplicações de TI sujeitas a riscos decorrentes da utilização de TI. Quando o auditor identificou aplicações de TI sujeitas a riscos decorrentes de TI, outros aspetos do ambiente de TI (por exemplo, base de dados, sistema operativo, rede) são suscetíveis de ser identificados porque tais aspetos suportam e interagem com as aplicações de TI identificadas.

Identificação dos riscos decorrentes da utilização de TI e controlos gerais de TI (Ref: Parágrafo 26 c)

O apêndice 6 apresenta considerações para a compreensão dos controlos gerais de TI.

A173. Ao identificar os riscos decorrentes da utilização de TI, o auditor pode considerar a natureza da aplicação de TI identificada ou outro aspeto do ambiente de TI e as razões para estar sujeita a riscos decorrentes da utilização de TI. Para algumas aplicações de TI identificadas ou outros aspetos do ambiente de TI, o auditor pode identificar os riscos aplicáveis decorrentes da utilização de TI que se relacionam principalmente com acesso não autorizado ou alterações de programas não autorizadas, bem como os que abordam riscos relacionados com alterações inadequadas de dados (por exemplo, o risco de alterações inadequadas nos dados através do acesso direto à base de dados ou a capacidade de manipular diretamente a informação).

A174. A extensão e a natureza dos riscos aplicáveis decorrentes da utilização das TI variam consoante a natureza e as características das aplicações de TI identificadas e outros aspetos do ambiente de TI. Os riscos de TI aplicáveis podem resultar de quando a entidade utiliza prestadores de serviços externos ou internos para aspetos específicos do seu ambiente de TI (por exemplo, subcontratar o alojamento do seu ambiente de TI a terceiros ou, num grupo, utilizar um centro de serviços partilhados para a gestão centralizada dos processos de TI). Também podem também ser identificados riscos aplicáveis decorrentes da utilização de TI relacionados com a cibersegurança. É mais provável que venham a existir mais riscos decorrentes da utilização de TI quando o volume ou a complexidade dos controlos automatizados das aplicações for maior e o órgão de gestão estiver a depositar uma confiança maior nesses controlos para o processamento eficaz das transações ou para a manutenção eficaz da integridade das informações subjacentes.

Avaliação da conceção e determinação da implementação dos controlos identificados na componente das atividades de controlo (Ref: Parágrafo 26(d))

A175. A avaliação da conceção de um controlo identificado implica a consideração do auditor sobre se o controlo, individualmente ou em combinação com outros controlos, é capaz de, de forma eficaz, prevenir, ou detetar e corrigir, as distorções materiais (ou seja, o objetivo de controlo).

A176. O auditor determina a implementação de um controlo identificado, confirmando que o controlo existe e que a entidade o utiliza. Não faz sentido o auditor avaliar a implementação de um controlo que não é concebido de forma eficaz. Consequentemente, o auditor avalia primeiro a conceção de um controlo. Um controlo mal concebido pode representar uma deficiência de controlo.

A177. Os procedimentos de avaliação dos riscos para obter provas de auditoria sobre a conceção e implementação de controlos identificados na componente das atividades de controlo podem incluir:

- Indagação ao pessoal da entidade.
- Observação da aplicação de controlos específicos.
- Inspecionar documentos e relatórios.

No entanto, a indagação por si só não é suficiente para tais fins.

A178. O auditor pode esperar, com base na experiência da auditoria anterior ou com base nos procedimentos de avaliação dos riscos do período corrente, que o órgão de gestão não tenha concebido ou implementado controlos de forma eficaz para fazer face a um risco significativo. Nesses casos, os procedimentos efetuados para dar resposta à exigência no parágrafo 26(d) podem consistir em determinar que esses controlos não foram concebidos ou implementados de forma eficaz. Se os resultados dos procedimentos indicarem que os controlos foram recentemente concebidos ou implementados, exige-se que o auditor execute os procedimentos previstos no parágrafo 26(b)-(d) sobre os controlos recentemente concebidos ou implementados.

A179. O auditor pode concluir que um controlo, que é concebido e implementado de forma eficaz, pode ser adequado para testar a fim de ter em conta a sua eficácia operacional na conceção de procedimentos substantivos. No entanto, quando um controlo não é concebido ou implementado de forma eficaz, não há qualquer benefício em testá-lo. Quando o auditor planeia testar um controlo, as informações obtidas sobre em que medida o controlo aborda os riscos de distorção material são um contributo para a avaliação, por parte do auditor, do risco de controlo ao nível da asserção.

A180. A avaliação da conceção e implementação dos controlos identificados na componente das atividades de controlo não é suficiente para testar a sua eficácia operacional. Todavia, para controlos automatizados, o auditor pode planear testar a eficácia operacional dos controlos automatizados através da identificação e teste dos controlos gerais de TI que preveem o funcionamento consistente de um controlo automatizado em vez de executar diretamente testes de eficácia operacional aos controlos automatizados. A obtenção de prova de auditoria sobre a implementação de um controlo manual num determinado momento não proporciona provas de auditoria sobre a eficácia operacional do controlo em outras ocasiões durante o período abrangido pela auditoria. Testes da eficácia operacional dos controlos, incluindo testes de controlos indiretos, são ainda descritos na ISA 330.[45]

A181. Quando o auditor planeia não testar a eficácia operacional dos controlos identificados, o conhecimento do auditor pode ainda assim ajudar na conceção da natureza, oportunidade e extensão dos procedimentos de auditoria substantivos que respondam aos riscos de distorção material relacionados.

> **Exemplo:**
>
> Os resultados destes procedimentos de avaliação do risco podem constituir uma base para que o auditor considere eventuais desvios numa população ao conceber amostras de auditoria.

Deficiências de controlo dentro do Sistema de Controlo Interno da Entidade (Ref: Parágrafo 27)

A182. Na realização das avaliações de cada uma das componentes do sistema de controlo interno da entidade,[46] o auditor pode determinar que certas políticas da entidade numa componente não são adequadas à natureza e circunstâncias da entidade. Tal determinação pode ser um indicador que ajuda o auditor a identificar deficiências de controlo. Se o auditor tiver identificado uma ou mais deficiências de controlo, o auditor pode considerar o efeito dessas deficiências de controlo na conceção de procedimentos de auditoria adicionais, em conformidade com a ISA 330.

A183. Se o auditor tiver identificado uma ou mais deficiências de controlo, a ISA 265[47] exige que o auditor determine se, individual ou em combinação, as deficiências constituem uma deficiência significativa. O auditor recorre ao julgamento profissional para determinar se uma deficiência representa uma deficiência de controlo significativa.[48]

> **Exemplos:**
>
> As circunstâncias que podem indiciar que existe uma deficiência de controlo significativa incluem matérias como:
>
> - Identificação de fraude de qualquer magnitude que envolva a gestão de topo;
> - Processos internos identificados que são inadequados relativos ao relato e comunicação de deficiências assinaladas pela auditoria interna;

[45] ISA 330, parágrafos 8-11
[46] Parágrafos 21 b, 22 b, 24 c, 25 c e 26 d
[47] ISA 265, *Comunicação de Deficiências no Controlo Interno aos Encarregados da Governação e ao Órgão de Gestão*, parágrafo 8
[48] ISA 265, os parágrafos A6-A7 estabelecem indicadores de deficiências significativas, e as matérias a considerar para determinar se uma deficiência, ou uma combinação de deficiências, no controlo interno constituem uma deficiência significativa.

- Deficiências comunicadas anteriormente que não são corrigidas em tempo útil pelo órgão de gestão;
- Falha do órgão de gestão em responder a riscos significativos, por exemplo, não implementando controlos sobre riscos significativos; e
- Alterações de demonstrações financeiras anteriormente emitidas.

Identificação e Avaliação dos Riscos de Distorção Material (Ref: Parágrafo 28-37)

Por que razão o auditor identifica e avalia os riscos de distorção material

A184. Os riscos de distorção material são identificados e avaliados pelo auditor a fim de determinar a natureza, oportunidade e extensão dos procedimentos de auditoria adicionais necessários para obter prova de auditoria adequadas e suficiente. Esta prova permite ao auditor emitir, com um nível aceitável de risco de auditoria, uma opinião- sobre as demonstrações financeiras.

A185. A informação recolhida através da realização de procedimentos de avaliação do risco é usada como prova de auditoria para proporcionar a base para a identificação e avaliação dos riscos de distorção material. Por exemplo, a prova de auditoria obtida na avaliação da conceção dos controlos identificados e na determinação de se esses controlos foram implementados na componente das atividades de controlo, é a usada como prova de auditoria para apoiar a avaliação do risco. Esta prova também constitui uma base para que o auditor conceba respostas globais para fazer face aos riscos avaliados de distorção material ao nível da demonstração financeira, bem como à conceção e realização de procedimentos de auditoria adicionais cuja natureza, calendário e extensão respondam aos riscos avaliados de distorção material ao nível da asserção, em conformidade com a ISA 330.

Identificação dos riscos de Distorção Material (Ref: Parágrafo 28)

A186. A identificação dos riscos de distorção material é efetuada antes da consideração de quaisquer controlos relacionados (isto é, o risco inerente), e baseia-se na consideração preliminar, por parte do auditor, das distorções que têm uma possibilidade razoável de ocorrerem e de serem materiais se vierem a ocorrer.[49]

A187. Identificar os riscos de distorção material também constitui a base para o auditor determinar as asserções relevantes, o que ajuda o auditor a determinar as classes de transações, saldos de contas e divulgações significativas.

Asserções

Por que razão o Auditor usa asserções

A188. Ao identificar e avaliar os riscos de distorção material, o auditor utiliza asserções para considerar os diferentes tipos de potenciais distorções que podem ocorrer. Asserções para as quais o auditor identificou riscos relacionados de distorção material são asserções relevantes.

O Uso de Asserções

A189. Ao identificar e avaliar os riscos de distorção material, o auditor pode usar as categorias de asserções descritas no parágrafo A190(a)-(b) abaixo ou pode expressá-las de forma diferente, desde que todos os aspetos descritos abaixo tenham sido abordados. O auditor pode optar por combinar as asserções sobre classes de transações e acontecimentos, e as divulgações relacionadas, com as asserções sobre saldos de contas e divulgações relacionadas.

A190. As asserções usadas pelo auditor para considerar os diferentes tipos de potenciais distorções que podem ocorrer podem classificar-se nas seguintes categorias:

(a) Asserções sobre classes de transações e acontecimentos, e divulgações relacionadas, para o período abrangido pela auditoria:

(i) Ocorrência — as transações e acontecimentos que foram registados ou divulgados ocorreram e tais transações e acontecimentos dizem respeito à entidade.

(ii) Plenitude — todas as transações e acontecimentos que deveriam ter sido registados foram registados, e todas as divulgações relacionadas que deveriam ter sido incluídas nas demonstrações financeiras foram incluídas.

[49] ISA 200, parágrafo A16

(iii) Rigor — quantias e outros elementos relativos a transações e acontecimentos registados foram registados apropriadamente e as divulgações relacionadas foram adequadamente mensuradas e descritas.

(iv) Corte — as transações e acontecimentos foram registados no período contabilístico correto.

(v) Classificação — as transações e acontecimentos foram registados nas contas apropriadas.

(vi) Apresentação — as transações e acontecimentos apropriadamente agregados ou desagregados e claramente descritos, e as divulgações relacionadas são relevantes e compreensíveis no contexto dos requisitos do referencial de relato financeiro aplicável.

(b) Asserções sobre saldos de contas e divulgações relacionadas, no final do período:

(i) Existência — os ativos, passivos e interesses de capital próprio existem.

(ii) Direitos e obrigações — a entidade detém ou controla os direitos sobre os ativos, e os passivos são obrigações da entidade.

(iii) Plenitude - todos os ativos, passivos e interesses de capital próprio que deveriam ter sido registados foram registados, e todas as divulgações relacionadas que deveriam ter sido incluídas nas demonstrações financeiras foram incluídas.

(iv) Rigor, valorização e imputação — os ativos, passivos e interesses de capital próprio foram incluídos nas demonstrações financeiras por quantias apropriadas e quaisquer ajustamentos de valorização ou de imputação foram apropriadamente registadas, e as divulgações relacionadas foram apropriadamente mensuradas e descritas.

(v) Classificação — os ativos, passivos e interesses de capital próprio foram registados nas contas apropriadas.

(vi) Apresentação — os ativos, passivos e interesses de capital próprio foram adequadamente agregados ou desagregados e claramente descritos, e as divulgações relacionadas são relevantes e compreensíveis no contexto dos requisitos do referencial de relato financeiro aplicável.

A191. As asserções descritas no parágrafo 190(a)-(b) acima, adaptadas conforme adequado, também podem ser usadas pelo auditor para considerar os diferentes tipos de distorções que podem ocorrer nas divulgações não diretamente relacionadas com classes de transações, e acontecimentos registados ou saldos de contas.

> **Exemplo**:
>
> Um exemplo de tal divulgação inclui quando pelo referencial de relato financeiro aplicável possa ser exigido à entidade que descreva a sua exposição aos riscos decorrentes de instrumentos financeiros, incluindo a forma como os riscos surgem; os objetivos, políticas e processos para gerir os riscos; e os métodos utilizados para mensurar os riscos.

Considerações Específicas para Entidades do Sector Público

A192. Ao fazer asserções sobre as demonstrações financeiras das entidades do sector público, para além das asserções constantes do parágrafo A190(a)-(b), o órgão de gestão pode frequentemente afirmar que as transações e acontecimentos foram realizados de acordo com a lei, regulamentos ou outra autoridade. Tais asserções podem enquadrar-se no âmbito da auditoria da demonstração financeira.

*Riscos de Distorção material ao Nível da Demonstração Financeira (*Ref: Parágrafos 28 (a) e 30)

Por que razão o Auditor Identifica e Avalia os Riscos de Distorção de Material ao Nível da Demonstração Financeira

A193. O auditor identifica os riscos de distorção material ao nível da demonstração financeira para determinar se os riscos têm um efeito profundo nas demonstrações financeiras, o que exigiria, consequentemente, uma resposta global em conformidade com a ISA 330.[50]

A194. Adicionalmente, os riscos de distorção material ao nível da demonstração financeira também podem afetar as asserções individuais, e a identificação destes riscos pode ajudar o auditor a avaliar os riscos de distorção material ao nível da asserção e na conceção de procedimentos de auditoria adicionais para fazer face aos riscos identificados.

[50] ISA 330, parágrafo 5

Identificar e Avaliar os Riscos de Distorção de Material ao Nível da Demonstração Financeira

A195. Os riscos de distorção material ao nível da demonstração financeira referem-se a riscos que se relacionam de forma mais profunda com as demonstrações financeiras como um todo e que potencialmente podem afetar muitas asserções. Os riscos desta natureza não são necessariamente riscos identificáveis com asserções específicas a nível da classe de transações, saldo de conta ou divulgação (por exemplo, risco de substituição de controlos pelo órgão de gestão). Pelo contrário, representam circunstâncias que podem aumentar profundamente os riscos de distorção material ao nível da asserção. A avaliação do auditor sobre se os riscos identificados se relacionam profundamente com as demonstrações financeiras apoia a avaliação do auditor sobre os riscos de distorção material ao nível da demonstração financeira. Em outros casos, uma série de asserções também podem ser identificadas como suscetíveis ao risco, podendo, consequentemente, afetar a identificação e avaliação dos riscos por parte do auditor sobre os riscos de distorção material ao nível da asserção.

Exemplo:

A entidade enfrenta perdas operacionais e problemas de liquidez e depende de financiamento que ainda não foi assegurado. Nesta circunstância, o auditor pode determinar que o pressuposto contabilístico da continuidade dá origem a um risco de distorção material ao nível da demonstração financeira. Nesta situação, o referencial contabilístico pode ter de ser aplicado usando uma base de liquidação, o que provavelmente afetaria todas as asserções de forma profunda.

A196. A identificação e avaliação por parte do auditor dos riscos de distorção material ao nível da demonstração financeira é influenciada pela compreensão do auditor sobre o sistema de controlo interno da entidade, nomeadamente a compreensão do auditor sobre o ambiente de controlo, o processo de avaliação de risco da entidade e o processo da entidade para monitorizar o sistema de controlo interno, e:

- Os resultados das avaliações relacionadas exigidas pelos parágrafos 21(b), 22(b), 24(c) e 25; e
- Quaisquer deficiências de controlo identificadas de acordo com o parágrafo 27.

Em especial, os riscos a nível da demonstração financeira podem resultar de deficiências no ambiente de controlo ou de acontecimentos ou condições externas, tais como condições económicas em declínio.

A197. Os riscos de distorção material por fraude podem ser particularmente relevantes para a consideração por parte do auditor dos riscos de distorção material ao nível da demonstração financeira.

Exemplo:

O auditor entende, a partir de indagações ao órgão de gestão, que as demonstrações financeiras da entidade são para serem usadas em discussões com os financiadores, a fim de garantir financiamento adicional para manter o fundo de maneio. O auditor pode, consequentemente, determinar que existe uma maior suscetibilidade a distorção devido a fatores de risco de fraude que afetam o risco inerente (isto é, a suscetibilidade das demonstrações financeiras a distorção material devido ao risco de relato financeiro fraudulento, como a sobreavaliação de ativos e receitas e a subavaliação de passivos e despesas, para assegurar que o financiamento será obtido).

A198. O entendimento do auditor, incluindo as avaliações relacionadas, do ambiente de controlo e de outros componentes do sistema de controlo interno pode levantar dúvidas sobre a capacidade do auditor de obter prova de auditoria para servir de base ao parecer de auditoria ou para que seja motivo para renunciar ao trabalho caso tal renúncia seja possível nos termos da legislação ou regulamentação aplicável.

Exemplos:

- Como resultado da avaliação do ambiente de controlo da entidade, o auditor tem preocupações com a integridade do órgão de gestão da entidade, que pode ser tão grave ao ponto de levar o auditor a concluir que o risco de distorção intencional, por parte do órgão de gestão, nas demonstrações financeiras é tal que não pode ser efetuada uma auditoria.
- Como resultado da avaliação do sistema de informação e comunicação da entidade, o auditor determina que mudanças significativas no ambiente de TI têm sido mal geridas, com pouca supervisão do órgão de gestão e dos encarregados da governação. O auditor conclui que existem preocupações significativas sobre a condição e a fiabilidade dos registos contabilísticos da entidade. Em tais

circunstâncias, o auditor pode determinar que é improvável que esteja disponível prova de auditoria adequada e suficiente para suportar uma opinião sem reservas sobre as demonstrações financeiras.

A199. A ISA 705 (Revista)[51] estabelece requisitos e proporciona orientações para determinar se existe necessidade de o auditor exprimir uma opinião com reservas (ou adversa) ou uma escusa de opinião ou, como é exigido em alguns casos, renunciar ao trabalho caso a renúncia seja possível nos termos da legislação ou regulamentação aplicável.

Considerações Específicas para Entidades do Sector Público

A200. Para as entidades do sector público, a identificação dos riscos ao nível da demonstração financeira pode incluir a consideração de matérias relacionadas com o ambiente político, o interesse público e sensibilidade do programa.

Riscos de Distorção Material no Nível da Asserção (Ref: Parágrafo 28(b))

O apêndice 2 apresenta exemplos, no contexto de fatores de risco inerente, de acontecimentos ou condições que podem indicar suscetibilidade a distorção que possa ser material.

A201. Os riscos de deturpações materiais que não se relacionam profundamente com as demonstrações financeiras são riscos de distorção material ao nível da asserção.

Asserções Relevantes e Classes de Transações, Saldos de Contas e Divulgações Significativas (Ref: Parágrafo 29)

Por que razão asserções significativas e classes significativas de transações, saldos de contas e divulgações são determinadas

A202. A determinação das asserções relevantes e das classes de transações, saldos de contas e divulgações significativas constitui a base para o âmbito da compreensão do auditor sobre o sistema de informação da entidade, a ser obtido em conformidade com o parágrafo 25(a). Este entendimento pode adicionalmente ajudar o auditor a identificar e avaliar os riscos de distorção material (ver A86).

Ferramentas e Técnicas Automatizadas

A203. O auditor pode utilizar técnicas automatizadas para ajudar na identificação de classes de transações, saldos de contas e divulgações significativas.

Exemplos:

- Uma população inteira de transações pode ser analisada usando ferramentas e técnicas automatizadas para entender a sua natureza, origem, tamanho e volume. Ao aplicar técnicas automatizadas, o auditor pode, por exemplo, identificar que uma conta com saldo nulo no final do período era composta por numerosas transações que se compensavam entre si e lançamentos de diário que ocorreram durante o período, indicando que o saldo da conta ou a classe de transações podem ser significativos (por exemplo, uma conta transitória de salários). Esta mesma conta transitória de salários também pode identificar os reembolsos de despesas ao órgão de gestão (e a outros colaboradores), que pode ser uma divulgação significativa devido a estes pagamentos serem feitos a partes relacionadas.
- Ao analisar os fluxos de uma população inteira de transações de receitas, o auditor pode identificar mais facilmente uma classe de transações significativa que não tinha sido identificada anteriormente.

Divulgações que Podem Ser Significativas

A204. As divulgações significativas incluem divulgações quer quantitativas quer qualitativas para as quais há uma ou mais asserções relevantes. Exemplos de divulgações que têm aspetos qualitativos e que podem ter asserções relevantes e que podem, portanto, ser consideradas significativas pelo auditor, incluem divulgações sobre:

- Liquidez e garantias de dívida de uma entidade em dificuldades financeiras.
- Acontecimentos ou circunstâncias que conduziram ao reconhecimento de uma perda por imparidade.
- Principais origens de incerteza de estimativa, incluindo pressupostos sobre o futuro.
- A natureza de uma alteração de uma política contabilística e de outras divulgações relevantes exigidas

[51] ISA 705 (Revista), *Alterações ao parecer no relatório do auditor independente*

pelo referencial de relato financeiro aplicável, quando, por exemplo, é expectável que novos requisitos de relato financeiro tenham um impacto significativo na posição financeira e no desempenho financeiro da entidade.

- Acordos de pagamento com base em ações, incluindo informação sobre como qualquer quantia reconhecida foi determinada, e outras divulgações relevantes.
- Partes relacionadas e transações entre partes relacionadas.
- Análise de sensibilidade, incluindo os efeitos de alterações nos pressupostos utilizados pela entidade em técnicas de avaliação com o objetivo de permitir aos utilizadores compreenderem a incerteza da subjacente da mensuração de uma quantia registada ou divulgada.

Avaliação dos Riscos de Distorção Material ao Nível da Asserção

Avaliação do Risco Inerente (Ref: Parágrafos 31-33)

Avaliação da probabilidade e magnitude da distorção (Ref: Parágrafo: 31)

Por que razão o auditor avalia a probabilidade e magnitude da distorção

A205. O auditor avalia a probabilidade e a magnitude da distorção para os riscos identificados de distorção material, uma vez que a importância da combinação da probabilidade de ocorrência de uma distorção e a magnitude da potencial distorção onde a distorção ocorra determinam onde, no espectro de risco inerente, o risco identificado é avaliado, o que informa o auditor sobre a necessidade de conceção de procedimentos adicionais de auditoria para fazer face ao risco.

A206. A avaliação do risco inerente de riscos identificados de distorção material também ajuda o auditor a determinar riscos significativos. O auditor determina riscos significativos porque são exigidas respostas específicas a riscos significativos em conformidade com a ISA 330 e outras ISA.

A207. Os fatores de risco inerente influenciam a avaliação pelo auditor da probabilidade e magnitude da distorção para os riscos identificados de distorção material ao nível da asserção. Quanto maior for o grau de suscetibilidade a distorção material de uma classe de transações, saldo de contas ou divulgação, mais provável é que o risco inerente avaliado seja mais alto. Considerar o grau em que os fatores de risco inerente afetam a suscetibilidade a distorção de uma asserção, ajuda o auditor a avaliar adequadamente o risco inerente para os riscos de distorção material ao nível da asserção e a conceber uma resposta mais precisa a esse risco.

Espectro de risco inerente

A208. Na avaliação do risco inerente, o auditor utiliza o julgamento profissional para determinar a importância da combinação da probabilidade e da magnitude de uma distorção.

A209. O risco inerente avaliado relativo a um risco específico de distorção ao nível da asserção representa um julgamento dentro de um intervalo, de mais baixo e para mais alto, no espectro de risco inerente. O julgamento sobre onde no intervalo se situa a avaliação do risco inerente pode variar em função da natureza, dimensão e complexidade da entidade, e tem em conta a avaliação da probabilidade e magnitude da distorção e os fatores de risco inerente.

A210. Ao considerar a probabilidade de uma distorção, o auditor considera a possibilidade de ocorrer uma distorção, tendo por base a consideração dos fatores de risco inerente.

A211. Ao considerar a magnitude de uma distorção, o auditor considera os aspetos qualitativos e quantitativos da eventual distorção (isto é, as distorções nas asserções sobre classes de transações, saldos de contas ou divulgações podem ser considerados materiais devido à dimensão, natureza ou circunstâncias).

A212. O auditor usa a importância da combinação da probabilidade e magnitude de uma eventual distorção na determinação de onde no espectro de risco inerente (ou seja, no intervalo) o risco inerente é avaliado. Quanto maior for a combinação da probabilidade e da magnitude, mais alto será o risco decorrente da avaliação do risco inerente; quanto mais baixa for a combinação da probabilidade e da magnitude, mais baixo será o risco decorrente da avaliação do risco inerente.

A213. Para que um risco seja avaliado como mais alto no espectro do risco inerente, não significa que quer a magnitude quer a probabilidade tenham de ser avaliadas como elevadas. Pelo contrário, é a intersecção da magnitude e probabilidade da distorção material no espectro do risco inerente que irá determinar se o risco que resulta da avaliação do risco inerente é mais alto ou mais baixo no espectro do risco inerente. Um risco inerente avaliado como mais alto também pode resultar de diferentes combinações de probabilidade e magnitude, por exemplo,

um risco inerente avaliado como mais alto pode resultar de uma menor probabilidade, mas de uma magnitude muito elevada.

A214. A fim de desenvolver estratégias adequadas para responder aos riscos de distorção material, o auditor pode classificar os riscos de distorção material dentro de categorias ao longo do espectro de risco inerente, com base na sua avaliação do risco inerente. Estas categorias podem ser descritas de diferentes formas. Independentemente do método de categorização utilizado, a avaliação do risco inerente pelo auditor é adequada quando a conceção e a aplicação de procedimentos de auditoria adicionais para fazer face aos riscos identificados de distorção material ao nível da asserção respondem adequadamente à avaliação do risco inerente e às razões dessa avaliação.

Riscos Generalizados de Distorção Material ao Nível da Asserção (Ref: Parágrafo 31(b))

A215. Ao avaliar os riscos identificados de distorção material ao nível da asserção, o auditor pode concluir que alguns riscos de distorção material se relacionam mais profundamente com as demonstrações financeiras como um todo e podem afetar potencialmente muitas asserções, caso em que o auditor pode atualizar a identificação dos riscos de distorção material ao nível da demonstração financeira.

A216. Nas circunstâncias em que os riscos de distorção material sejam identificados como riscos ao nível da demonstração financeira devido ao seu efeito profundo numa série de asserções, e sejam identificáveis com asserções específicas, exige-se que o auditor tenha em conta esses riscos ao avaliar o risco inerente para riscos de distorção material ao nível da asserção.

Considerações Específicas para Entidades do Sector Público

A217. No exercício do julgamento profissional sobre a avaliação do risco de distorção material, os auditores do sector público podem considerar a complexidade dos regulamentos e diretivas e os riscos de incumprimento com as autoridades.

Riscos Significativos (Ref: Parágrafo 32)

Por que razão os riscos significativos são identificados e as implicações para a auditoria

A218. A identificação de riscos significativos permite ao auditor concentrar mais atenção nos riscos que se encontram na parte superior do espectro de risco inerente, através da execução de determinadas respostas que são exigidas, incluindo:

- Exige-se que os controlos que respondam a riscos significativos sejam identificados de em conformidade com o parágrafo 26(a)(i), com a obrigação de avaliar se o controlo foi concebido de forma eficaz e implementado em conformidade com o parágrafo 26(d).
- A ISA 330 exige que os controlos que respondam a riscos significativos sejam testados no período atual (quando o auditor pretenda confiar da eficácia operacional de tais controlos) e que os procedimentos substantivos sejam planeados e executados de forma a responder especificamente ao risco significativo identificado.[52]
- A ISA 330 exige que o auditor obtenha provas de auditoria mais persuasivas quanto mais alto for o risco resultante da avaliação do risco feita pelo auditor.[53]
- A ISA 260 (Revista) exige comunicação com encarregados da governação sobre os riscos significativos identificados pelo auditor.[54]
- A ISA 701 exige que o auditor tenha em conta riscos significativos na determinação das matérias que requereram uma atenção significativa do auditor, que são matérias que podem ser matérias-chave para a auditoria.[55]
- Revisão atempadamente da documentação de auditoria pelo sócio responsável pelo trabalho nas fases adequadas durante a auditoria permite que matérias significativas, incluindo riscos significativos, sejam resolvidas atempadamente para a satisfação do sócio responsável pelo trabalho na data ou antes da data do relatório do auditor.[56]
- A ISA 600 (Revista) exige ao auditor do grupo que avalie a adequação da conceção e execução de

[52] ISA 330, parágrafos 15 e 21
[53] ISA 330, parágrafo 7(b)
[54] ISA 260 (Revista), parágrafo 15
[55] ISA 701, *Comunicação de principais matérias de auditoria no Relatório do Auditor Independente*, parágrafo 9
[56] ISA 220 (Revista), parágrafos 32 e A87 a A89

procedimentos de auditoria adicionais para áreas em que se avaliou um risco mais elevado de distorções materiais nas demonstrações financeiras do grupo, ou riscos significativos, nos quais um auditor da componente está a determinar os procedimentos de auditoria adicionais a.[57]

Determinação de riscos significativos

A219. Ao determinar riscos significativos, o auditor pode identificar em primeiro lugar os riscos avaliados de distorção material que tenham sido avaliados como mais altos no espectro do risco inerente para constituir a base para considerar quais os riscos que podem estar próximos do limite superior. Estarem perto do limite superior do espectro de risco inerente diferirá de entidade para entidade, e não será necessariamente o mesmo em cada período na mesma entidade. Pode depender da natureza e das circunstâncias da entidade para a qual o risco está a ser avaliado.

A220. A determinação de quais os riscos que foram avaliados como de distorção material que estão próximos do limite superior do espectro de risco inerente e que, por essa razão, são riscos significativos, é uma questão de julgamento profissional, a menos que o risco seja de uma natureza especificada como para ser tratado como um risco significativo de acordo com os requisitos de outra ISA. A ISA 240 proporciona requisitos e orientações adicionais em relação à identificação e avaliação dos riscos de distorção material devido a fraude.[58]

Exemplo:

- O dinheiro num retalhista de supermercados seria normalmente considerado como estando sujeito a uma elevada probabilidade de potencial distorção (devido ao risco de desvio de dinheiro), no entanto, a magnitude seria normalmente muito baixa (devido aos baixos níveis de dinheiro físico manuseado nas lojas). A combinação destes dois fatores no espectro do risco inerente é improvável resulte em dinheiro vir a ser considerado como um risco significativo.
- Uma entidade está em negociações para vender um segmento de negócio. O auditor considera o efeito sobre a imparidade do *goodwill* e pode determinar que existe uma maior probabilidade de potencial distorção e maior magnitude devido ao impacto de fatores de risco inerente de subjetividade, incerteza e suscetibilidade ao enviesamento do órgão de gestão ou a outros fatores de risco de fraude. Isto pode resultar na imparidade do *goodwill* vir a ser considerada como um risco significativo.

A221. O auditor também tem em conta os efeitos relativos dos fatores de risco inerentes à avaliação do risco inerente. Quanto menor for o efeito dos fatores de risco inerente, maior é a probabilidade de o risco avaliado ser mais baixo. Os riscos de distorção material que podem ser avaliados como tendo um risco inerente mais alto e que podem, por essa razão, ser considerados como um risco significativo, podem resultar de matérias como:

- Transações para as quais existem múltiplos tratamentos contabilísticos aceitáveis de tal forma que haja subjetividade envolvida.
- Estimativas contabilísticas que têm elevada incerteza de estimativa ou modelos complexos.
- Complexidade na recolha e processamento de dados para suportar saldos de conta.
- Saldos de conta ou divulgações quantitativas que envolvem cálculos complexos.
- Princípios contabilísticos que podem estar sujeitos a interpretações diferentes.
- Alterações no negócio da entidade que envolvem alterações na contabilidade, por exemplo, fusões e aquisições.

Riscos para os quais procedimentos substantivos por si só não proporcionam prova de auditoria adequada e suficiente (Ref: Parágrafo 33)

Por que razão se exige que sejam identificados os riscos para os quais os procedimentos substantivos por si só não proporcionam e prova de auditoria adequada e suficiente

A222. Devido à natureza de um risco de distorção material, e às atividades de controlo que abordam esse risco, em algumas circunstâncias, a única forma de obter prova de auditoria adequadas e suficiente é testar a eficácia operacional dos controlos. Consequentemente, exige-se que o auditor identifique r todos esses riscos devido às implicações para a conceção e realização de procedimentos de auditoria adicionais, em conformidade com a ISA 330, para fazer face aos riscos de distorção material ao nível da asserção.

[57] ISA 600 (Revista), parágrafo 42
[58] ISA 240, parágrafos 26 a 28

A223. O parágrafo 26(a) (a) (iii) também exige a identificação de controlos que abordem riscos para os quais os procedimentos substantivos por si só não conseguem proporcionar prova de auditoria adequada, porque é exido ao auditor que, em conformidade com a ISA 330,[59] conceba e efetue testes a esses controlos.

Determinação dos riscos para os quais os procedimentos substantivos por si só não proporcionam prova de auditoria adequada e suficiente

A224. Quando as transações negócio de rotina estiverem sujeitas a um processamento altamente automatizado com pouca ou nenhuma intervenção manual, pode não ser possível executar apenas procedimentos substantivos em relação ao risco. Tal pode acontecer em circunstâncias em que uma quantidade significativa de informações de uma entidade seja iniciada, registada, processada ou reportada apenas sob forma eletrónica, como num sistema de informação que envolva um elevado grau de integração de todas as suas aplicações informáticas. Em tais casos:

- A prova de auditoria pode estar disponível apenas sob forma eletrónica, e a sua suficiência e adequação geralmente dependem da eficácia dos controlos sobre o seu rigor e plenitude.
- O potencial para iniciação ou alteração inadequada de informações ocorrerem e não serem detetadas pode ser maior se os controlos adequados não estiverem a funcionar eficazmente.

Exemplo:

Normalmente, não é possível obter prova de auditoria adequada e suficiente relativa às receitas de uma entidade de telecomunicações baseada apenas em procedimentos substantivos. Isto porque a evidência do telefonema ou atividade de dados não existe de uma forma que seja observável. Em vez disso, normalmente são realizados testes substanciais aos controlos para determinar se a atividade de origem e conclusão dos telefonemas, e dos dados é corretamente capturada (por exemplo, minutos de um telefonema ou volume de um *download*) e corretamente registada no sistema de faturação da entidade.

A225. A ISA 540 (Revista) proporciona orientações adicionais relacionadas com estimativas contabilísticas sobre riscos para os quais os procedimentos substantivos por si só não proporcionam prova de auditoria adequada e suficiente.[60] Em relação às estimativas contabilísticas, isto pode não se limitar a processamentos automatizados, mas pode também ser aplicável a modelos complexos.

Avaliação do Risco de Controlo (Ref: Parágrafo 34)

A226. Os planos do auditor para testar a eficácia operacional dos controlos baseiam-se na expectativa de que os controlos estão a funcionar eficazmente, o que constituirá a base da avaliação do risco de controlo por parte do auditor. A expectativa inicial da eficácia operacional dos controlos baseia-se na avaliação da conceção e na determinação da implementação dos controlos identificados na componente das atividades de controlo, feitas pelo auditor. Uma vez testada a eficácia operacional dos controlos em conformidade com a ISA 330, o auditor poderá confirmar a expectativa inicial sobre a eficácia operacional dos controlos. Se os controlos não estiverem a funcionar eficazmente como esperado, então o auditor terá de rever a avaliação do risco de controlo em conformidade com o parágrafo 37.

A227. A avaliação do risco de controlo pelo auditor pode ser efetuada de diferentes formas, dependendo das técnicas ou metodologias preferenciais de auditoria, podendo ser expressa de diferentes formas.

A228. Se o auditor planeia testar a eficácia operacional dos controlos, pode ser necessário testar uma combinação de controlos para confirmar a expectativa do auditor de que os controlos estão a funcionar eficazmente. O auditor pode planear testar os controlos diretos e indiretos, incluindo os controlos gerais de TI, e, se assim for, ter em conta o efeito combinado esperado dos controlos na avaliação do risco de controlo. Na medida em que o controlo a testar não responda totalmente o risco inerente avaliado, o auditor determina as implicações na conceção de procedimentos de auditoria adicionais para reduzir o risco de auditoria a um nível aceitável.

A229. Quando o auditor planeia testar a eficácia operacional de um controlo automatizado, o auditor também pode planear testar a eficácia operacional dos controlos gerais relevantes de TI que suportam o funcionamento contínuo desse controlo automatizado para fazer face aos riscos decorrentes da utilização de TI e proporcionar uma base para a expectativa do auditor de que o controlo automatizado funcionou eficazmente durante o período. Quando o auditor espera que os controlos gerais de TI relacionados sejam ineficazes, esta determinação pode afetar a avaliação, pelo auditor, do risco de controlo ao nível da asserção e os procedimentos de auditoria

[59] ISA 330, parágrafo 8
[60] ISA 540 (Revista), parágrafos A87 a A89

adicionais do auditor podem ter de incluir procedimentos substantivos para responder aos riscos aplicáveis decorrentes da utilização das TI. As orientações adicionais sobre os procedimentos que o auditor pode executar nestas circunstâncias são fornecidas na ISA 330.[61]

Avaliação da Prova de Auditoria Obtida A Partir dos Procedimentos de Avaliação do Risco (Ref: Parágrafo 35)

Por que razão o Auditor avalia a prova de auditoria obtida a partir dos procedimentos de avaliação do risco

A230. A prova de auditoria obtida a partir da realização de procedimentos de avaliação do risco constitui a base para a identificação e avaliação dos riscos de distorção material. Isto proporciona a base para a conceção, por parte do auditor, da natureza, oportunidade e extensão dos procedimentos de auditoria adicionais que respondam aos riscos avaliados de distorção material ao nível da asserção, em conformidade com a ISA 330. Consequentemente, a prova de auditoria obtida a partir dos procedimentos de avaliação do risco constitui uma base para a identificação e avaliação dos riscos de distorção material, quer devido a fraude quer devido a erro, aos níveis da demonstração financeira e da asserção.

Avaliação da Prova de Auditoria

A231. A prova de auditoria obtida a partir dos procedimentos de avaliação de riscos compreendem tanto informações que suportam e corroboram as asserções d do órgão de gestão, como qualquer informação que contradiga tais asserções.[62]

Ceticismo profissional

A232. Ao avaliar a prova de auditoria obtida a partir dos procedimentos de avaliação do risco, o auditor considera se foi obtida compreensão suficiente sobre a entidade e o seu ambiente, o referencial de relato financeiro aplicável e o sistema de controlo interno da entidade, para poder identificar os riscos de distorção material, bem como se existe qualquer prova que seja contraditória que possa indicar um risco de erro de distorção material.

Classes de Transações, Saldos de Conta e Divulgações que Não São Significativas, mas Que São Materiais (Ref: Parágrafo 36)

A233. Tal como explicado na ISA 320,[63] a materialidade e o risco de auditoria são tidos em conta na identificação e avaliação dos riscos de distorção material em classes de transações, saldos de contas e divulgações. A determinação da materialidade pelo auditor é uma questão de julgamento profissional e é afetada pela perceção que o auditor tem sobre as necessidades de informação financeira dos utilizadores das demonstrações financeiras. [64] Para efeitos da presente ISA e do parágrafo 18 da ISA 330, as classes de transações, saldos de contas ou divulgações são materiais se omitirem, distorcerem ou tornarem pouco claras informações sobre elas que possam razoavelmente influenciar as decisões económicas dos utilizadores tomadas com base nas demonstrações financeiras como um todo.

A234. Pode haver classes de transações, saldos de contas ou divulgações que sejam materiais, mas não tenham sido consideradas classes de transações, saldos de contas ou divulgações significativas (ou seja, não existem asserções relevantes identificadas).

> **Exemplo**:
>
> A entidade pode ter uma divulgação sobre a remuneração dos executivos para a qual o auditor não identificou um risco de distorção material. Todavia, o auditor pode determinar que esta divulgação é material baseado nas considerações do parágrafo A233.

A235. Os procedimentos de auditoria para tratar classes de transações, saldos de contas ou divulgações que sejam materiais, mas que não sejam considerados como sendo significativos, são abordados na ISA 330. [65] Quando uma classe de transações, saldo ou divulgação de conta é considerada como significativa conforme exigido pelo parágrafo 29, a classe de transações, saldo de conta ou divulgação também é uma classe de transações, saldo de conta ou divulgação material para efeitos do parágrafo 18 da ISA 330.

Revisão da Avaliação do Risco (Ref: Parágrafo 37)

A236. Durante a auditoria, podem chegar ao conhecimento do auditor informações novas ou outras que diferem

[61] ISA 330, parágrafos A29 a A31
[62] ISA 500, parágrafo A5
[63] ISA 320, parágrafo A1
[64] ISA 320, parágrafo 4
[65] ISA 330, parágrafo 18

significativamente das informações nas quais se baseou a avaliação do risco.

> **Exemplo**:
>
> A avaliação de risco da entidade pode basear-se na expectativa de que determinados controlos estão a funcionar eficazmente. Na execução de testes a esses controlos, o auditor pode obter prova de auditoria de que não estavam a funcionar eficazmente em momentos relevantes durante a auditoria. Do mesmo modo, na execução de procedimentos substantivos, o auditor pode detetar erros em quantias ou frequências maiores do que os que são consistentes com as avaliações de risco do auditor. Em tais circunstâncias, a avaliação do risco pode não refletir adequadamente as verdadeiras circunstâncias da entidade e os procedimentos de auditoria adicionais planeados podem não ser eficazes na deteção de distorções materiais. Os parágrafos 16 e 17 da ISA 330 proporcionam orientações adicionais para avaliar a eficácia operacional dos controlos.

Documentação (Ref: Parágrafo 38)

A237. Para auditorias recorrentes, determinada documentação pode ser transportada d para o exercício seguinte, atualizada conforme necessário para refletir alterações no negócio ou nos processos da entidade.

A238. A ISA 230 refere, entre outras considerações, que embora possa não existir uma única forma de documentar o exercício do ceticismo profissional pelo auditor, a documentação de auditoria pode, no entanto, proporcionar prova do exercício de ceticismo profissional por parte do auditor. [66] Por exemplo, quando a prova de auditoria obtida a partir dos procedimentos de avaliação do risco inclui prova que corrobora e contradiz as asserções do órgão de gestão, a documentação pode incluir a forma como o auditor avaliou essa prova, incluindo os julgamentos profissionais efetuados na avaliação de se a prova da auditoria constitui uma base adequada para a identificação e avaliação, por parte do auditor, dos riscos de distorção. Os exemplos de outros requisitos nesta ISA para os quais a documentação pode proporcionar prova do exercício do ceticismo profissional por parte do auditor incluem:

- O Parágrafo 13, que exige que o auditor conceba e execute procedimentos de avaliação de risco de uma forma que não seja enviesada com vista à obtenção de prova de auditoria que possa corroborar a existência de riscos ou com vista à exclusão de prova de auditoria que possa contradizer a existência de riscos;
- O Parágrafo 17, que requer uma discussão entre os membros chave da equipa de trabalho sobre o referencial de relato financeiro aplicável e sobre a suscetibilidade das demonstrações financeiras da entidade a distorção material;
- Os Parágrafos 19(b) e 20, que exigem que o auditor obtenha uma compreensão das razões para quaisquer alterações às políticas contabilísticas da entidade e avalie se as políticas contabilísticas da entidade são adequadas e consistentes com o referencial de relato financeiro aplicável;
- Os Parágrafos 21(b), 22(b), 23(b), 24(c), 25 (c), 26(d) e 27, que exigem ao auditor que avalie, com base no entendimento exigido obtido, se as componentes do sistema de controlo interno da entidade são adequadas às circunstâncias da entidade, tendo em conta a natureza e a complexidade da entidade, e que determine se foram identificadas uma ou mais deficiências de controlo;
- O Parágrafo 35, que exige que o auditor tenha em conta toda a prova de auditoria obtida a partir dos procedimentos de avaliação do risco, quer corroborativa quer contraditória com as asserções feitas pelo órgão de gestão, e avale se a prova de auditoria obtida a partir dos procedimentos de avaliação do risco proporcionam uma base adequada para a identificação e avaliação dos riscos de distorção material;
- O Parágrafo 36, que exige que o auditor avalie, quando aplicável, se a determinação, por parte do auditor, de que não existem riscos de distorção material para uma classe de transações, saldo de conta ou divulgação material continua a ser adequada.

Escalabilidade

A239. A forma como os requisitos do parágrafo 38 são documentados é determinada pelo auditor usando julgamento profissional.

A240. Documentação mais pormenorizada, suficiente para permitir que um auditor experiente, sem experiência prévia com a auditoria, compreenda a natureza, oportunidade e extensão dos procedimentos de auditoria realizados, pode ser necessária para suportar a fundamentação dos julgamentos difíceis efetuados.

---

[66] ISA 230, parágrafo A7

A241. Para as auditorias de entidades menos complexas, a forma e extensão da documentação podem ser simples e relativamente concisas. A forma e extensão da documentação do auditor é influenciada pela natureza, dimensão e complexidade da entidade e pelo seu sistema de controlo interno, pela disponibilidade de informação por parte da entidade e pela metodologia de auditoria e tecnologia utilizada no decurso da auditoria. Não é necessário documentar a totalidade do conhecimento do auditor sobre a entidade e as matérias que lhe estão relacionadas. Os elementos-principais[67] do conhecimento documentados pelo auditor podem incluir aqueles nos quais o auditor baseou a avaliação dos riscos de distorção material. No entanto, não se exige que o auditor documente todos os fatores de risco inerente que foram tidos em conta na identificação e avaliação dos riscos de distorção material ao nível da asserção.

Exemplo:

Nas auditorias de entidades menos complexas, a documentação de auditoria pode ser incorporada na documentação, por parte do auditor, da estratégia global e do plano de auditoria. [68] Do mesmo modo, por exemplo, os resultados da avaliação do risco podem ser documentados separadamente ou podem ser documentados como parte da documentação, por parte do auditor, dos procedimentos de auditoria adicionais.[69]

[67] ISA 230, parágrafo 8
[68] ISA 300, *Planeamento de uma Auditoria de Demonstrações Financeiras*, parágrafos 7, 9 e A13
[69] ISA 330, parágrafo 28

Apêndice 1

(Ref: Para. A61-A67)

Considerações para a Compreensão da Entidade e do seu Modelo de Negócio

Este apêndice explica os objetivos e o âmbito do modelo de negócio da entidade e fornece exemplos de matérias que o auditor pode considerar na compreensão das atividades da entidade que podem ser incluídas no modelo de negócio. A compreensão do auditor sobre o modelo de negócio da entidade e a forma como é afetada pela sua estratégia de negócio e pelos seus objetivos comerciais, pode ajudar o auditor a identificar riscos empresariais que possam ter um efeito nas demonstrações financeiras. Além disso, isto pode ajudar o auditor a identificar os riscos de distorção material.

Objetivos e Âmbito do Modelo de Negócio de uma Entidade

1. O modelo de negócio de uma entidade descreve como uma entidade considera, por exemplo, a sua estrutura organizacional, operações ou âmbito de atividades, linhas de negócio (incluindo concorrentes e clientes dos mesmos), processos, oportunidades de crescimento, globalização, requisitos regulamentares e tecnologias. O modelo de negócio da entidade descreve como a entidade cria, preserva e capta valor financeiro ou mais amplo, para os seus *stakeholders*.

2. Estratégias são as abordagens através das quais a gestão planeia atingir os objetivos da entidade, incluindo a forma como a entidade planeia endereçar os riscos e oportunidades que enfrenta. As estratégias de uma entidade são alteradas ao longo do tempo pela gestão, para responder às mudanças nos seus objetivos e nas circunstâncias internas e externas em que opera.

3. Uma descrição de um modelo de negócio inclui tipicamente:

   - O âmbito das atividades da entidade e por que as faz.
   - A estrutura da entidade e a escala das suas operações.
   - Os mercados ou esferas geográficas ou demográficas, e partes da cadeia de valor, em que opera, a forma como se envolve com esses mercados ou esferas (principais produtos, segmentos de clientes e métodos de distribuição), e a base em que concorre.
   - Os processos empresariais ou operacionais da entidade (por exemplo, processos de investimento, financiamento e exploração) utilizados na realização das suas atividades, focando-se nas partes dos processos de negócio que são importantes na criação, preservação ou captação de valor.
   - Os recursos (por exemplo, financeiros, humanos, intelectuais, ambientais e tecnológicos) e outros *inputs* e relações (por exemplo, clientes, concorrentes, fornecedores e colaboradores) que são necessários ou importantes para o seu sucesso.
   - Como o modelo de negócio da entidade integra a utilização de TI nas suas interações com clientes, fornecedores, credores e outras partes interessadas através de interfaces de TI e outras tecnologias.

4. Um risco comercial pode ter consequências imediatas para o risco de erros materiais para classes de transações, saldos de contas e divulgações ao nível da asserção ou ao nível da demonstração financeira. Por exemplo, o risco de negócio decorrente de uma queda significativa dos valores do mercado imobiliário pode aumentar o risco de distorção material associada à asserção de valorização para um mutuante de empréstimos imobiliários de médio prazo. No entanto, o mesmo risco, nomeadamente em conjugação com uma grave recessão económica que simultaneamente aumenta o risco subjacente de perdas de crédito ao longo da vida nos seus empréstimos, pode também ter uma consequência a longo prazo. A exposição líquida resultante a perdas de crédito pode levantar dúvidas significativas sobre a capacidade da entidade de operar no pressuposto da continuidade. Em caso afirmativo, isso poderá ter implicações para a gestão e para a conclusão do auditor quanto à adequação do uso pela entidade do pressuposto contabilístico da continuidade e à determinação quanto a se existe uma incerteza material. Por conseguinte, a determinação sobre se um risco de negócio pode resultar num risco de distorção material é, por essa razão, considerado tendo em conta as circunstâncias da entidade. Exemplos de acontecimentos e condições que podem dar origem à existência de riscos de distorção material são indicados no **apêndice 2**.

Atividades da Entidade

5. Exemplos de matérias que o auditor pode considerar ao obter um entendimento das atividades da entidade (incluídas no modelo de negócio da entidade) incluem:

(a) Operações comerciais tais como:

- Natureza das fontes de receita, produtos ou serviços e mercados, incluindo o envolvimento no comércio eletrónico, como vendas na Internet e atividades de marketing.
- Condução de operações (por exemplo, fases e métodos de produção, ou atividades expostas a riscos ambientais).
- Alianças, empreendimentos conjuntos e atividades de outsourcing.
- Dispersão geográfica e segmentação da indústria.
- Localização de instalações de produção, armazéns e escritórios, e localização e quantidades de inventários.
- Clientes chave e importantes fornecedores de bens e serviços, acordos de emprego (incluindo a existência de contratos sindicais, pensões e outros benefícios pós-emprego, *opções de ações* ou acordos de bónus de incentivo, e regulação governamental relacionada com questões laborais).
- Atividades e despesas de pesquisa e desenvolvimento.
- Transações com partes relacionadas.

(b) Investimentos e atividades de investimento tais como:

- Aquisições ou alienações planeadas ou recentemente executadas.
- Investimentos e vendas de títulos e empréstimos.
- Atividades de investimento de capital.
- Investimentos em entidades não consolidadas, incluindo parcerias não controladas, empreendimentos conjuntos e entidades com fins especiais não controladas.

(c) Financiamento e atividades de financiamento, tais como:

- Estrutura de propriedade de grandes subsidiárias e entidades associadas, incluindo estruturas consolidadas e não consolidadas.
- Estrutura da dívida e termos conexos, incluindo acordos de financiamento fora do balanço e acordos de locação financeira.
- Beneficiários proprietários (por exemplo, locais, estrangeiros, reputação e experiência de negócios) e partes relacionadas.
- Uso de instrumentos financeiros derivados.

Natureza das Entidades com Finalidade Especial

6. Uma entidade com finalidade especial (por vezes designada como veículo com finalidade especial) é uma entidade criada geralmente para fins reduzidos e bem definidos, tais como a realização de uma locação ou uma titularização de ativos financeiros ou a realização de atividades de investigação e desenvolvimento. Pode assumir a forma de uma empresa, trust, parceria ou entidade sem personalidade jurídica. A entidade em nome da qual a entidade com finalidade especial foi criada pode muitas vezes transferir ativos para esta última (por exemplo, como parte de uma transação de desreconhecimento envolvendo ativos financeiros), obter o direito de utilizar os ativos deste último, ou realizar serviços para estes últimos, enquanto outras partes podem fornecer o financiamento a esta última. Como a ISA 550 indica, em algumas circunstâncias, uma entidade com finalidade especial pode ser uma parte relacionada da entidade.[70]

7. As estruturas de relato financeiro especificam frequentemente condições pormenorizadas destinadas a determinar o controlo, ou circunstâncias em que a entidade especial deve ser considerada para consolidação. A interpretação dos requisitos dessas estruturas de relato exige frequentemente um conhecimento pormenorizado dos acordos relevantes que envolvem a entidade com finalidade especial.

[70] ISA 550, parágrafo A7

Apêndice 2

(Ref: Para. 12(f), 19(c), A7-A8, A85-A89)

Compreensão de fatores de risco inerentes

Este apêndice fornece uma explicação adicional sobre os fatores de risco inerentes, bem como as questões que o auditor pode considerar na compreensão e aplicação dos fatores de risco inerentes na identificação e avaliação dos riscos de distorções materiais ao nível das asserções.

Os Fatores de Risco Inerentes

1. Os fatores de risco inerentes são características de acontecimentos ou condições que afetam a suscetibilidade a distorção de uma asserção sobre uma classe de transações, saldo de conta ou divulgação, seja por fraude ou erro, e antes de serem tidos em conta os controlos. Tais fatores podem ser qualitativos ou quantitativos e incluem complexidade, subjetividade, alteração, incerteza ou suscetibilidade a distorção devido a preconceitos da gestão ou outros fatores de risco de fraude,[71] na medida em que afetem o risco inerente. Ao obter a compreensão da entidade e do seu ambiente, bem como a estrutura de relato financeiro aplicável e as políticas contabilísticas da entidade, nos termos dos parágrafos 19 (a)-(b), o auditor compreende também como os fatores de risco inerentes afetam a suscetibilidade das asserções a distorções na elaboração das demonstrações financeiras.

2. Os fatores de risco inerentes relativos à preparação das informações exigidas pela estrutura de relato financeiro aplicável (referidas no presente número como "informações necessárias") incluem:

   - *Complexidade* - surge quer da natureza da informação, quer da forma como as informações necessárias são preparadas, incluindo quando os respetivos processos de preparação são mais inerentemente difíceis de aplicar. Por exemplo, pode surgir complexidade:
     - No cálculo da estimativa dos descontos a obter dos fornecedores, porque pode ser necessário ter em conta diferentes termos comerciais com muitos fornecedores diferentes, ou muitas condições comerciais interrelacionadas que são todas relevantes no cálculo dos descontos devidos; ou
     - Quando existem muitas fontes de dados potenciais, com características diferentes utilizadas na elaboração de uma estimativa contabilística, o tratamento desses dados envolve muitas etapas interrelacionadas, pelo que os dados são inerentemente mais difíceis de identificar, capturar, aceder, compreender ou processar.
   - *Subjetividade* - decorre de limitações inerentes à capacidade de preparar as informações necessárias de forma objetiva, devido a limitações na disponibilidade de conhecimentos ou informações, de modo que a gestão possa ter de fazer uma eleição ou um juízo subjetivo sobre a abordagem adequada a seguir e sobre as informações resultantes a incluir nas demonstrações financeiras. Devido a diferentes abordagens para a preparação das informações necessárias, os diferentes resultados poderiam resultar da aplicação adequada dos requisitos da estrutura de relato financeiro aplicável. À medida que as limitações de conhecimento ou dados aumentam, a subjetividade nos julgamentos que podem ser feitos por indivíduos razoavelmente conhecedores e independentes, e a diversidade nos eventuais resultados desses julgamentos, também aumentará.
   - *Alteração* - resulta de eventos ou condições que, ao longo do tempo, afetam o negócio da entidade ou os aspetos económicos, contabilísticos, regulamentares, industriais ou outros aspetos do ambiente em que opera, quando os efeitos desses eventos ou condições se refletem na informação necessária. Tais eventos ou condições podem ocorrer durante ou entre períodos de relato financeiro. Por exemplo, a alteração pode resultar da evolução dos requisitos da estrutura de relato financeiro aplicável, ou da entidade e do seu modelo de negócio, ou no ambiente em que a entidade opera. Tal alteração pode afetar os pressupostos e julgamentos da gestão, incluindo no que diz respeito à seleção, pela gestão, das políticas contabilísticas ou à forma como são feitas as estimativas contabilísticas ou como as respetivas divulgações são apuradas.
   - *Incerteza* - surge quando as informações necessárias não podem ser preparadas com base apenas em dados suficientemente precisos e abrangentes que sejam verificáveis através de observação direta. Nestas circunstâncias, pode ser necessário adotar uma abordagem que aplique os conhecimentos disponíveis

[71] ISA 240, parágrafos A24-A27

para preparar as informações utilizando dados observáveis suficientemente precisos e abrangentes, na medida em que estes estejam disponíveis, e pressupostos razoáveis apoiados pelos dados disponíveis mais adequados, quando aqueles não estejam disponíveis. Os constrangimentos à disponibilidade de conhecimentos ou dados, que não estão sob o controlo da gestão (sujeito a restrições de custos, se for caso disso) são fontes de incerteza e os seus efeitos na preparação das informações necessárias não podem ser eliminados. Por exemplo, a incerteza da estimativa surge quando o montante monetário necessário não pode ser determinado com precisão e o resultado da estimativa não é conhecido antes da data em que as demonstrações financeiras são finalizadas.

- *Suscetibilidade a distorção devido a preconceitos de gestão ou outros fatores de risco de fraude, na medida em que afetam o risco inerente* – Suscetibilidade a preconceitos da gestão, resulta de condições que criam suscetibilidade à falha intencional ou não intencional por parte da gestão em manter a neutralidade na preparação da informação. O preconceito da gestão está muitas vezes associado a determinadas condições que têm o potencial de dar origem a que a gestão não mantenha a neutralidade ao exercer julgamento (indicadores de potenciais preconceitos da gestão), que poderiam levar a uma distorção material da informação que seria fraudulenta, se intencional. Estes indicadores incluem incentivos ou pressões na medida em que afetam o risco inerente (por exemplo, como resultado da motivação para alcançar um resultado desejado tal como um objetivo de lucro desejado ou rácio de capital), e a oportunidade para não manter a neutralidade. Os fatores relevantes para a suscetibilidade à distorção devido a fraude sob a forma de relato financeiro fraudulento ou apropriação indevida de ativos são descritos nos parágrafos A1 a A5 da ISA 240.

3. Quando a complexidade é um fator de risco inerente, pode haver uma necessidade inerente de processos mais complexos na preparação da informação, e tais processos podem ser inerentemente mais difíceis de aplicar. Como resultado, a sua aplicação pode requerer competências ou conhecimentos especializados, e pode exigir a utilização de um perito em gestão.

4. Quando o julgamento da gestão é mais subjetivo, a suscetibilidade a erros devido a preconceitos de gestão, quer não intencionais quer intencionais, pode igualmente aumentar. Por exemplo, a gestão pode ter de exercer um julgamento significativo na elaboração de estimativas contabilísticas identificadas como tendo uma elevada incerteza de estimativa e as conclusões relativas a métodos, dados e pressupostos podem refletir um enviesamento não intencional ou intencional por parte da gestão.

Exemplos de eventos ou condições que podem dar origem à existência de riscos de distorção de material

5. Seguem-se exemplos de acontecimentos (incluindo transações) e condições que podem indicar a existência de riscos de distorção material nas demonstrações financeiras, ao nível da demonstração financeira ou ao nível de asserção. Os exemplos fornecidos pelo fator de risco inerente abrangem uma vasta gama de eventos e condições; no entanto, nem todos os eventos e condições são relevantes para cada compromisso da auditoria e a lista de exemplos não está necessariamente completa. Os acontecimentos e condições foram categorizados pelo fator de risco inerente que pode ter o maior efeito nas circunstâncias. Importante, devido às inter-relações entre fatores de risco inerentes, os eventos e condições exemplo também são suscetíveis de ser sujeitos ou afetados, em diferentes graus, por outros fatores de risco inerentes.

Fator de risco inerente relevante:	Exemplos de Eventos ou Condições Que Podem Indicar a Existência de Riscos de Distorção Material ao Nível da Asserção:
Complexidade	Regulamentar: • Operações sujeitas a um elevado grau de regulação complexa. Modelo de negócio: • Existência de alianças e de empreendimentos conjuntos complexos Estrutura de relato financeiro aplicável: • Mensurações contabilísticas que envolvem processos complexos. Transações: • Utilização de financiamentos fora do balanço, entidades com finalidade especial e outras modalidades de financiamento complexas.

Fator de risco inerente relevante:	Exemplos de Eventos ou Condições Que Podem Indicar a Existência de Riscos de Distorção Material ao Nível da Asserção:
Subjetividade	Estrutura de relato financeiro aplicável: • Uma vasta gama de critérios possíveis para medir uma estimativa contabilística. Por exemplo, o reconhecimento pela gestão de amortizações ou de receitas e despesas de construção. • A seleção pela gestão de uma técnica ou modelo de avaliação para um ativo não corrente, tal como propriedades de investimento.
Alteração	Condições económicas: • Operações em regiões economicamente instáveis, por exemplo, países com desvalorização monetária significativa ou economias altamente inflacionárias. Mercados: • Operações expostas a mercados voláteis, por exemplo, negociação de futuros. Perda de cliente: • Preocupações de continuidade e liquidez, incluindo perda de clientes significativos. Modelo da indústria: • Mudanças na indústria em que a entidade opera. Modelo de negócio: • Alterações na cadeia de abastecimento. • Desenvolver ou oferecer novos produtos ou serviços, ou mudar-para novas linhas de negócio.
	Geografia: • Expansão para novos locais. Estrutura de entidade: • Alterações na entidade, tais como grandes aquisições ou reorganizações ou outros eventos incomuns. • Entidades ou segmentos de negócio com intenção de serem vendidos. Competência em recursos humanos: • Mudanças no pessoal-chave, incluindo a saída de executivos-chave. IT: • Alterações no ambiente de TI. • Instalação de novos sistemas de TI significativos relacionados com o relato financeiros. Estrutura de relato financeiro aplicável: • Aplicação de novas diretrizes contabilísticos. Capital: • Novos constrangimentos à disponibilidade de capital e crédito. Regulamentar: • Início de investigações sobre as operações ou resultados financeiros da entidade por organismos reguladores ou governamentais.

Fator de risco inerente relevante:	Exemplos de Eventos ou Condições Que Podem Indicar a Existência de Riscos de Distorção Material ao Nível da Asserção:
	• Impacto da nova legislação relacionada com a proteção do ambiente.
Incerteza	Relato: • Eventos ou transações que envolvam incertezas significativas de mensuração, incluindo estimativas contabilísticas e divulgações relacionadas. • Litígios pendentes e passivos contingentes, por exemplo, garantias de venda, garantias financeiras e recuperação ambiental.
Suscetibilidade a distorção devido a preconceitos da gestão ou outros fatores de risco de fraude na medida em que afetem o risco inerente	Relato: • Oportunidades para a administração e os colaboradores se envolverem em reportes financeiros fraudulentos, incluindo omissão, ou ocultação de informações significativas nas divulgações. Transações: • Transações significativas com partes relacionadas. • Montante significativo de transações não rotineiras ou não sistemáticas, incluindo transações entre empresas do grupo e grandes transações de receitas no final do período. • Transações que registadas com base na intenção da administração, por exemplo, no refinanciamento da dívida, nos ativos a serem vendidos e na classificação de títulos negociáveis.

Outros eventos ou condições que possam indicar riscos de distorção material ao nível da demonstração financeira:

- Falta de pessoal com competências adequadas de contabilidade e de reporte financeiro.
- Deficiências de controlo – particularmente no ambiente de controlo, no processo de avaliação de riscos e no processo de monitorização, e especialmente aqueles controlos que não são abordados pela gestão.
- Erros passados, histórico de erros ou uma quantidade significativa de ajustamentos no final do período.

Apêndice 3

(Ref: Parágrafos12(m), 21–26, A90–A181))

Compreender o Sistema de Controlo Interno da Entidade

1. O sistema de controlo interno da entidade pode refletir-se nos manuais de política e procedimentos, nos sistemas e formulários, bem como na informação incorporada neles, e é efetuado por pessoas. O sistema de controlo interno da entidade é implementado pela administração, pelos responsáveis pela governação e por outras pessoas com base na estrutura da entidade. O sistema de controlo interno da entidade pode ser aplicado com base nas decisões da gestão, dos responsáveis pela governação ou de outro pessoal e, no contexto de requisitos legais ou regulamentares, ao modelo operacional da entidade, à estrutura da entidade jurídica, ou a uma combinação destes.

2. Este apêndice explica mais detalhadamente os componentes bem como as limitações do sistema de controlo interno da entidade conforme apresentados nos parágrafos 12(m), 21 a 26 e A90 a A181, no contexto de uma auditoria de demonstrações financeiras.

3. Incluídos no sistema de controlo interno da entidade estão aspetos relacionados com os objetivos de reporte da entidade, incluindo os seus objetivos de relato financeiro, mas também podem incluir aspetos relacionados com as suas operações ou objetivos de conformidade, quando tais aspetos são relevantes para o relato financeiro.

> **Exemplo**:
>
> Os controlos sobre o cumprimento das leis e regulamentos podem ser relevantes para o relato financeiro quando esses controlos forem relevantes para a elaboração da divulgação de contingências nas demonstrações financeiras por parte da entidade.

Componentes do Controlo Interno

Ambiente de Controlo

4. O ambiente de controlo inclui as funções de governação e gestão e as atitudes, consciência e ações dos responsáveis pela governação e pela gestão relativamente ao sistema de controlo interno da entidade, e a sua importância na entidade. O ambiente de controlo define o tom de uma organização, influenciando a consciência de controlo das suas pessoas, e fornece a base global para o funcionamento dos outros componentes do sistema de controlo interno da entidade.

5. A consciência de controlo de uma entidade é influenciada pelos responsáveis pela governação, porque uma das suas funções é contrabalançar as pressões sobre a gestão em relação ao relato financeiro que possam decorrer de exigências de mercado ou de regimes de remuneração. A eficácia da conceção do ambiente de controlo em relação à participação dos responsáveis pela governação é, por conseguinte, influenciada por questões como:

   - A sua independência da gestão e a sua capacidade de avaliar as ações da gestão.
   - Se compreendem as transações comerciais da entidade.
   - Até que ponto avaliam se as demonstrações financeiras são preparadas de acordo com a estrutura de relato financeiro aplicável, incluindo se as demonstrações financeiras incluem divulgações adequadas.

6. O ambiente de controlo compreende os seguintes elementos:

   (a) *Como as responsabilidades da gestão são exercidas, tais como a criação e manutenção da cultura da entidade e a demonstração do compromisso da gestão com a integridade e os valores éticos*. A eficácia dos controlos não se pode sobrepor à integridade e valores éticos das pessoas que os criam, administram e monitorizam. A integridade e o comportamento ético são produto dos padrões ou códigos de conduta éticos e de comportamento da entidade, da forma como são comunicados (por exemplo, através de políticas), e de como se lhes dá força na prática (ex: através de ações do órgão de gestão para eliminar ou atenuar os incentivos ou tentações que possam levar o pessoal a empreender ações desonestas, ilegais ou que não sejam éticas). A comunicação das políticas da entidade relativas à integridade e valores éticos pode incluir a comunicação de padrões de comportamento ao pessoal através de políticas e códigos de conduta e através do exemplo.

   (b) *Quando os responsáveis pela governação são separados da gestão, como é que os responsáveis pela governação demonstram a independência da gestão e exercem a supervisão do sistema de controlo interno da entidade.* A consciência de controlo de uma entidade é influenciada por aqueles encarregados

da governação. As considerações podem incluir se existem indivíduos suficientes independentes da gestão e objetivos nas suas avaliações e tomadas de decisão; como os responsáveis pela governação identificam e aceitam responsabilidades de supervisão e se os responsáveis pela governação mantêm a responsabilidade de supervisão pela conceção, implementação e condução do sistema de controlo interno da entidade. A importância das responsabilidades dos encarregados da governação é reconhecida em códigos de conduta e outras leis e regulamentos ou orientações produzidas para o benefício dos próprios encarregados da governação. Outras responsabilidades dos encarregados da governação incluem a supervisão da conceção e do funcionamento eficaz de procedimentos de denúncia.

(c) *Como a entidade atribui autoridade e responsabilidade na prossecução dos seus objetivos.* Isto pode incluir considerações sobre:

- Áreas chave de autoridade e de responsabilidade e linhas apropriadas de relato.
- Políticas relativas a práticas de negócio apropriadas, aos conhecimentos e experiência do pessoal-chave e aos recursos proporcionados para o cumprimento das diferentes funções. e
- Políticas e comunicações com vista a assegurar que todo o pessoal entende os objetivos da entidade, sabe como as suas ações individuais se inter-relacionam e contribuem para esses objetivos e reconhece como e porquê serão responsabilizados.

(d) *Como a entidade atrai, desenvolve e retém indivíduos competentes em alinhamento com os seus objetivos.* Isto inclui como a entidade garante que os indivíduos têm o conhecimento e as competências necessárias para realizar as tarefas que definem o trabalho do indivíduo, por exemplo:

- Padrões para o recrutamento do pessoal mais qualificado – com uma ênfase nas habilitações académicas, experiência profissional anterior, referências passadas e evidência de integridade e comportamento ético.
- Políticas de formação que comunicam papéis e responsabilidades futuras e incluindo práticas como seminários e escolas de formação que ilustrem níveis esperados de desempenho e de comportamento, e
- Avaliações periódicas do desempenho que impulsionam promoções que demonstrem o compromisso da entidade na passagem do pessoal qualificado para níveis mais elevados de responsabilidade.

(e) *A forma como a entidade responsabiliza os indivíduos pelas suas responsabilidades na prossecução dos objetivos do sistema de controlo interno da entidade.* Isto pode ser realizado através de, por exemplo:

- Mecanismos de comunicação e responsabilização das pessoas pelo desempenho das responsabilidades de controlo e pela implementação de ações corretivas, se necessário;
- Estabelecer medidas de desempenho, incentivos e recompensas para os responsáveis pelo sistema de controlo interno da entidade, incluindo a forma como as medidas são avaliadas e manter a sua relevância;
- Como as pressões associadas à realização dos objetivos de controlo têm impacto nas responsabilidades e medidas de desempenho do indivíduo; e
- Como os indivíduos são disciplinados se necessário.

A adequação das matérias acima referidas será diferente para cada entidade, dependendo da sua dimensão, da complexidade da sua estrutura e da natureza das suas atividades.

O Processo da Entidade para Avaliação do Risco

7. O processo de avaliação de risco da entidade é um processo iterativo para identificar e analisar riscos para atingir os objetivos da entidade, e constitui a base para a forma como a gestão ou os responsáveis pela governação determinam os riscos a gerir.

8. Para efeitos de relato financeiro, o processo da entidade para avaliação do risco inclui a forma como o órgão de gestão identifica os riscos de negócio relevantes para a preparação de demonstrações financeiras de acordo com o referencial de relato financeiro aplicável, estima a sua importância, avalia a probabilidade da sua ocorrência e decide sobre as medidas de gestão desses riscos, bem como os respetivos resultados. Por exemplo, o processo da entidade para avaliação do risco pode abordar a forma como esta prevê a possibilidade de existirem transações não registadas ou identifica e analisa estimativas significativas registadas nas demonstrações financeiras.

9. Os riscos relevantes para um relato financeiro fiável incluem acontecimentos externos e internos, transações ou circunstâncias que possam ocorrer e que afetem adversamente a capacidade da entidade para iniciar, registar, processar e relatar informação financeira consistente com as asserções do órgão de gestão nas demonstrações financeiras. O órgão de gestão pode implementar planos, programas ou medidas para abordar riscos específicos, ou pode decidir assumir um determinado risco por razões de custo ou outras considerações. Os riscos podem surgir ou alterar-se devido a circunstâncias como:

- *Alterações no ambiente operacional.* Alterações no ambiente regulador económico ou operacional podem resultar em alterações das pressões competitivas e em riscos significativamente diferentes.
- *Novo pessoal.* O novo pessoal pode ter uma visão ou um entendimento diferentes do sistema de controlo interno da entidade.
- *Sistemas de informação novos ou reformulados.* Alterações significativas e rápidas nos sistemas de informação podem alterar o risco relativo ao sistema de controlo interno da entidade.
- *Crescimento rápido.* A expansão significativa e rápida das operações pode afetar os controlos e aumentar o risco de falhas nos controlos.
- *Nova tecnologia.* A incorporação de novas tecnologias nos processos de produção ou os sistemas de informação podem alterar o risco associado ao sistema de controlo interno da entidade.
- *Novos modelos de negócio, produtos ou atividades.* A entrada da entidade em novas áreas de negócio ou transações relativamente às quais a entidade tem pouca experiência pode introduzir novos riscos associados ao sistema de controlo interno da entidade.
- *Reestruturações empresariais.* As reestruturações podem ser acompanhadas por reduções de pessoal e alterações na supervisão e segregação de funções, que podem alterar o risco associado ao sistema de controlo interno da entidade.
- *Expansão de operações no estrangeiro.* A expansão ou aquisição de unidades operacionais no estrangeiro traz consigo novos riscos e, muitas vezes, riscos específicos que podem afetar o controlo interno, como por exemplo riscos adicionais ou alterados decorrentes das transações em moeda estrangeira.
- *Novas diretrizes contabilísticas.* A adoção de novos princípios contabilísticos ou a alteração de princípios contabilísticos existentes pode afetar os riscos na preparação de demonstrações financeiras.
- *Uso de Tecnologias de Informação (TI).* Riscos relativos:
  - Manter a integridade do tratamento de dados e informação;
  - Riscos para a estratégia de negócio da entidade que surgem se a estratégia de TI da entidade não apoiar eficazmente a estratégia de negócio da entidade; ou
  - Alterações ou interrupções no ambiente de TI ou no volume de negócios do pessoal de TI ou quando a entidade não efetue as atualizações necessárias ao ambiente de TI ou essas atualizações não são efetuadas atempadamente.

Processo da Entidade para Monitorizar o Sistema de Controlo Interno

10. O processo da entidade para monitorizar o sistema de controlo interno é um processo contínuo para avaliar a eficácia do sistema de controlo interno da entidade e para tomar as ações corretivas necessárias atempadamente. O processo de monitorização do sistema de controlo interno da entidade pode consistir em atividades em curso, avaliações separadas (realizadas periodicamente) ou alguma combinação dos dois. As atividades de monitorização em curso são muitas vezes integradas nas atividades recorrentes normais de uma entidade e podem incluir atividades regulares de gestão e supervisão. O processo da entidade provavelmente variará no âmbito e na frequência, dependendo da avaliação dos riscos por parte da entidade.

11. Os objetivos e o âmbito das funções de auditoria interna incluem normalmente atividades destinadas a avaliar ou monitorizar a eficácia do sistema de controlo interno da entidade[72]. O processo da entidade para monitorizar o sistema de controlo interno da entidade pode incluir atividades como a verificação pelo órgão de gestão de que as reconciliações bancárias estão a ser preparadas em tempo oportuno, a avaliação pelos auditores internos do cumprimento pelo pessoal de vendas das políticas da entidade relativas aos termos dos contratos de vendas

[72] ISA 610 (Revista 2013) e Apêndice 4 desta ISA fornecem mais orientações relacionadas com auditoria interna.

e a supervisão pelo departamento jurídico do cumprimento das políticas da entidade em termos de ética e de práticas de negócio. A monitorização é também efetuada para assegurar que os controlos continuem a operar de forma eficaz ao longo do tempo. Por exemplo, se a frequência e o rigor das reconciliações bancárias não forem monitorizados, é provável que o pessoal deixe de as preparar.

12. Os controlos relacionados com o processo da entidade para monitorizar o sistema de controlo interno da entidade, incluindo os que monitorizam os controlos automatizados subjacentes, podem ser automatizados ou manuais, ou uma combinação de ambos. Por exemplo, uma entidade pode utilizar controlos automatizados de monitorização sobre o acesso a determinadas tecnologias com relatórios automatizados de atividade invulgar para a gestão, que investigam manualmente anomalias identificadas.

13. Ao distinguir entre uma atividade de monitorização e um controlo relacionado com o sistema de informação, são considerados os pormenores subjacentes da atividade, especialmente quando a atividade envolve algum nível de revisão da supervisão. As revisões de supervisão não são automaticamente classificadas como atividades de monitorização e pode ser uma questão de julgamento se uma revisão é classificada como um controlo relacionado com o sistema de informação ou uma atividade de monitorização. Por exemplo, a intenção de um controlo mensal de plenitude seria detetar e corrigir erros, onde uma atividade de monitorização perguntaria por que razão estão a ocorrer erros e atribuiria à gestão a responsabilidade de corrigir o processo para evitar erros futuros. Em termos simples, um controlo relacionado com o sistema de informação responde a um risco específico, enquanto uma atividade de monitorização avalia se os controlos dentro de cada um dos cinco componentes do sistema de controlo interno da entidade estão a funcionar conforme pretendido.

14. As atividades de monitorização podem incluir o uso de informação proveniente de comunicações de entidades externas que possam indicar problemas ou evidenciar áreas que necessitam de melhoria. Os clientes corroboram de forma implícita a faturação ao procederem ao pagamento das faturas ou ao reclamar quanto aos débitos que lhes foram efetuados. Adicionalmente, os reguladores podem comunicar com a entidade em relação a matérias que afetam o funcionamento do sistema de controlo interno da entidade, como por exemplo comunicações respeitantes a inspeções efetuadas por agências reguladoras do setor bancário. Igualmente, ao executar atividades de monitorização, o órgão de gestão pode considerar quaisquer comunicações dos auditores externos relativas ao sistema de controlo interno da entidade.

O Sistema de Informação e Comunicação

15. O sistema de informação relevante para a elaboração das demonstrações financeiras consiste em atividades e políticas, bem como registos contabilísticos e de apoio, concebidos e estabelecidos para:

- Iniciar, registar e processar as transações de entidades (bem como capturar, processar e divulgar informações sobre eventos e condições que não as transações) e manter a responsabilidade pelos ativos, passivos e capitais próprios conexos;
- Resolver o processamento incorreto de transações, por exemplo, seguimento dos ficheiros e procedimentos automatizados suspensos para limpar os itens suspensos em tempo oportuno;
- Processar e anotar situações em que o sistema substitui ou contorna os controlos;
- Incorporar informações provenientes do processamento de transações no livro-razão geral (por exemplo, transferência de transações acumuladas a partir de um livro-razão subsidiário);
- Capturar e processar informação de eventos e condições, que não as transações, relevante para a elaboração das demonstrações financeiras, tais como a depreciação e a amortização de ativos e alterações na recuperabilidade dos ativos; e
- Assegurar que as informações que a estrutura de relato financeiro aplicável requer que sejam divulgadas, são acumuladas, registadas, processadas, resumidas e adequadamente relatadas nas demonstrações financeiras.

16. Os processos de negócio de uma entidade incluem as atividades concebidas para:

- Desenvolver, comprar, produzir, vender e distribuir os produtos e serviços de uma entidade;
- Garantir o cumprimento das leis e regulamentos; e
- Registar Informações, incluindo informações contabilísticas e de relato financeiro.

Os processos de negócio resultam nas transações que são registadas, processadas e comunicadas pelo sistema de informação.

17. A qualidade da informação afeta a capacidade da administração de tomar decisões adequadas na gestão e controlo das atividades da entidade e na elaboração de relatórios financeiros fiáveis.

18. A comunicação, que implica proporcionar a compreensão das funções e responsabilidades individuais relativas ao sistema de controlo interno da entidade, pode assumir formas como manuais de políticas, manuais de contabilidade e financeiros e memorandos. A comunicação também pode ser feita eletronicamente, oralmente, e através das ações de gestão.

19. A comunicação por parte da entidade das funções e responsabilidades de reporte financeiro e de questões significativas relacionadas com o relato financeiro implica proporcionar uma compreensão das funções e responsabilidades individuais relativas ao sistema de controlo interno relevante para o relato financeiro da entidade. Pode incluir questões como a medida em que o pessoal compreende como é que as suas atividades no sistema de informação se relacionam com o trabalho de outros e os meios de reportar exceções a um nível superior adequado dentro da entidade.

Atividades de controlo

20. Os controlos na componente das atividades de controlo são identificados em conformidade com o parágrafo 26. Esses controlos incluem controlos de processamento de informação e controlos gerais de TI, os quais podem ser de natureza manual ou automatizada. Quanto maior for a extensão dos controlos automatizados, ou dos controlos que envolvem aspetos automatizados que a gestão utiliza e nos quais confia em relação ao seu relato financeiro, mais importante poderá tornar-se para a entidade implementar controlos gerais de TI que abordem o funcionamento contínuo dos aspetos automatizados dos controlos de processamento da informação. Os controlos na componente das atividades de controlo podem pertencer ao seguinte:

- *Autorização e aprovações.* Uma autorização afirma que uma transação é válida (ou seja, representa um acontecimento económico real ou está dentro da política de uma entidade). Uma autorização normalmente assume a forma de uma aprovação por um nível mais elevado da gestão ou de uma verificação e determinação se a transação é válida. Por exemplo, um supervisor aprova um relatório de despesas depois de analisar se as despesas parecem razoáveis e dentro da política. Um exemplo de uma aprovação automatizada é quando um custo unitário da fatura é automaticamente comparado com o custo unitário da ordem de compra relacionada dentro de um nível de tolerância pré-estabelecido. As faturas dentro do nível de tolerância são automaticamente aprovadas para pagamento. Aquelas faturas fora do nível de tolerância são sinalizadas para uma investigação adicional.

- *Reconciliações* – As reconciliações comparam dois ou mais elementos de dados. Se forem identificadas diferenças, serão tomadas medidas para que os dados fiquem de acordo. As reconciliações geralmente abordam a plenitude ou a exatidão das transações de processamento.

- *Verificações* – As verificações comparam dois ou mais itens entre si ou comparam um item com uma política, e provavelmente envolverão uma ação de seguimento quando os dois itens não correspondem ou o item não é consistente com a política. As verificações geralmente abordam a plenitude, exatidão ou validade das transações de processamento.

- *Controlos físicos ou lógicos, incluindo aqueles que abordam a segurança dos bens contra acesso, aquisição, utilização ou alienação não autorizados.* Controlos que englobam:

    - A segurança física dos bens, incluindo salvaguardas adequadas, tais como instalações seguras em relação ao acesso a bens e registos.

    - A autorização de acesso a programas informáticos e ficheiros de dados (isto é, acesso lógico).

    - A contagem periódica e a comparação com os valores apresentados nos registos de controlo (por exemplo, comparando os resultados das contagens de caixa, títulos e inventário com os registos contabilísticos).

A medida em que os controlos físicos destinados a evitar o roubo de ativos são relevantes para a fiabilidade da preparação das demonstrações financeiras depende de circunstâncias tais como se os ativos são altamente suscetíveis a apropriação indevida.

- *Segregação de funções.* Atribuir a diferentes pessoas as responsabilidades de autorizar transações, registar transações e manter a custódia dos ativos. A segregação de funções destina-se a reduzir as oportunidades de permitir que qualquer pessoa esteja em condições de cometer e ocultar erros ou fraudes no decurso normal das funções da pessoa.

Por exemplo, um gestor que autorize a venda de crédito não é responsável pela manutenção de registos a receber ou manuseamento de recebimentos. Se uma pessoa for capaz de realizar todas estas atividades, a pessoa poderia, por exemplo, criar uma venda fictícia que poderia passar despercebida. Do mesmo modo, os vendedores não devem ter a capacidade de modificar ficheiros de preços do produto ou taxas de comissão.

Por vezes, a segregação não é prática, rentável ou exequível. Por exemplo, entidades mais pequenas e menos complexas podem não ter recursos suficientes para alcançar a segregação ideal, e o custo da contratação de pessoal adicional pode ser proibitivo. Nestas situações, a gestão pode instituir controlos alternativos. No exemplo acima, se o vendedor pode modificar os ficheiros de preços do produto, uma atividade de controlo de deteção pode ser colocada em prática de forma que pessoal não relacionado com a função de vendas reveja periodicamente se e em que circunstâncias o vendedor alterou os preços.

21. Certos controlos podem depender da existência de controlos de supervisão adequados estabelecidos pela gestão ou pelos responsáveis pela governação. Por exemplo, os controlos de autorização podem ser delegados ao abrigo de orientações estabelecidas, tais como critérios de investimento definidos pelos responsáveis pela governação; alternativamente, transações não rotineiras, tais como grandes aquisições ou alienações, podem exigir uma aprovação específica de alto nível, incluindo, em alguns casos, a dos acionistas.

Limitações do Controlo Interno

22. O sistema de controlo interno da entidade, por mais eficaz que seja, pode fornecer a uma entidade apenas segurança razoável sobre a consecução dos objetivos de relato financeiro da entidade. A probabilidade da realização é afetada pelas limitações inerentes ao controlo interno. Estas incluem as realidades de que o julgamento humano na tomada de decisões pode ser incorreto e de que podem ocorrer falhas no sistema de controlo interno da entidade devido a erros humanos. Por exemplo, pode haver um erro na conceção ou na mudança de um controlo. Do mesmo modo, o funcionamento de um controlo pode não ser eficaz, como quando as informações produzidas para efeitos do sistema de controlo interno da entidade (por exemplo, um relatório de exceção) não são efetivamente utilizadas porque o indivíduo responsável pela revisão das informações não compreende o seu propósito ou não toma as medidas adequadas.

23. Além disso, os controlos podem ser contornados pelo conluio de duas ou mais pessoas ou pela gestão passar por cima dos controlos. Por exemplo, a gestão pode celebrar acordos paralelos com clientes que alterem os termos e condições dos contratos de venda padrão da entidade, o que pode resultar num reconhecimento indevido de receitas. Além disso, verificações, com direito de edição, numa aplicação de TI destinada a identificar e reportar transações que excedam os limites de crédito especificados podem levar à ultrapassagem ou à desativação destes limites.

24. Além disso, na conceção e implementação dos controlos, a gestão pode fazer julgamentos sobre a natureza e extensão dos controlos que escolhe implementar, bem como na natureza e extensão dos riscos que escolhe assumir.

Apêndice 4

(Ref: Parágrafos 14(a), 24(a)(ii), A25–A28, A118))

Considerações para a Compreensão da Função de Auditoria Interna de uma Entidade

Este apêndice fornece mais considerações relativas à compreensão da função de auditoria interna da entidade quando tal função existe.

Objetivos e Âmbito da Função de Auditoria Interna

1. Os objetivos e âmbito de uma função de auditoria interna, a natureza das suas responsabilidades e o seu estatuto no seio da organização, incluindo a autoridade e responsabilização da função, variam muito e dependem da dimensão, complexidade e estrutura da entidade e dos requisitos da gestão e, se for caso disso, dos responsáveis pela governação. Estas questões podem ser definidas numa carta de auditoria interna ou em termos de referência.

2. As responsabilidades de uma função de auditoria interna podem incluir a execução de procedimentos e a avaliação dos resultados para dar segurança à gestão e aos responsáveis pela governação no que respeita à conceção e eficácia da gestão dos riscos, ao sistema de controlo interno e aos processos de governação da entidade. Se for o caso, a função de auditoria interna pode desempenhar um papel importante no processo da entidade para monitorizar o sistema de controlo interno da entidade. No entanto, as responsabilidades da função de auditoria interna podem centrar-se na avaliação da economia, eficiência e eficácia das operações e, nesse caso, o trabalho da função de auditoria interna pode não estar diretamente relacionado com o relato financeiro da entidade.

Inquéritos da Função de Auditoria Interna

3. Se uma entidade tiver uma função de auditoria interna, os inquéritos às pessoas adequadas dentro da função podem fornecer informações úteis ao auditor na obtenção de um entendimento da entidade e do seu ambiente, da estrutura de relato financeiro aplicável e do sistema de controlo interno da entidade, bem como na identificação e avaliação dos riscos de distorção material aos níveis da demonstração financeira e da asserção. No exercício do seu trabalho, é provável que a função de auditoria interna tenha obtido informações sobre as operações e riscos comerciais da entidade, podendo ter conclusões baseadas no seu trabalho, tais como deficiências ou riscos de controlo identificados, que possam fornecer contributos valiosos para a compreensão do auditor sobre a entidade e o seu ambiente, a estrutura de relato financeiro aplicável, o sistema de controlo interno da entidade, as avaliações de risco do auditor ou outros aspetos da auditoria. Por conseguinte, procede-se a inquéritos do auditor independentemente de o auditor ter ou não a expetativa de utilizar o trabalho da função de auditoria interna para modificar a natureza ou o calendário, ou reduzir a extensão dos procedimentos de auditoria a realizar[73]. Os inquéritos de particular relevância podem ser sobre questões que a função de auditoria interna levantou com os responsáveis pela governação e os resultados do processo de avaliação de risco da própria função de auditoria interna.

4. Se, com base nas respostas aos inquéritos ao auditor, parecerem existirem conclusões que podem ser relevantes para o relato financeiro da entidade e para a auditoria das demonstrações financeiras, o auditor pode considerar adequado ler os relatórios relacionados da função de auditoria interna. Exemplos de relatórios da função de auditoria interna que podem ser relevantes incluem os documentos da estratégia e planeamento da função de auditoria interna e os relatórios que foram preparados para a gestão ou para os responsáveis pela governação descrevendo as conclusões dos exames da função de auditoria interna.

5. Além disso, em conformidade com a ISA 240[74], se a função de auditoria interna fornecer informações ao auditor sobre qualquer fraude efetiva, suspeita ou alegada, o auditor toma isso em consideração na identificação pelo auditor do risco de distorção material por fraude.

6. Os indivíduos adequados no âmbito da função de auditoria interna com quem são feitos inquéritos são aqueles que, no julgamento do auditor, possuem os conhecimentos, experiência e autoridade adequados, tais como o diretor executivo da auditoria interna ou, dependendo das circunstâncias, outros funcionários dentro da função de auditoria interna. O auditor pode igualmente considerar oportuno realizar reuniões periódicas com estes indivíduos.

---

[73] Os requisitos relevantes estão contidos na ISA 610 (Revisão 2013).

[74] ISA 240, parágrafo 19

Consideração da Função de Auditoria Interna na Compreensão do Ambiente de Controlo

7. Ao compreender o ambiente de controlo, o auditor pode considerar a forma como a gestão respondeu às conclusões e recomendações da função de auditoria interna relativas a deficiências de controlo identificadas relevantes para a preparação das demonstrações financeiras, incluindo se e como essas respostas foram implementadas e se foram posteriormente avaliadas pela função de auditoria interna.

Compreender o Papel que a Função de Auditoria Interna desempenha no Processo de Monitorização do Sistema de Controlo Interno

8. Se a natureza das responsabilidades e as atividades de garantia da função de auditoria interna estiverem relacionadas com o relato financeiro da entidade, o auditor poderá igualmente utilizar o trabalho da função de auditoria interna para modificar a natureza ou o calendário, ou reduzir a extensão dos procedimentos de auditoria a executar diretamente pelo auditor na obtenção de provas de auditoria. Os auditores podem ser mais suscetíveis de utilizar o trabalho da função de auditoria interna de uma entidade quando pareça, por exemplo, com base na experiência em auditorias anteriores ou nos procedimentos de avaliação de risco do auditor, que a entidade tem uma função de auditoria interna que tem recursos adequados e apropriados à complexidade da entidade e à natureza das suas operações, e tem uma relação de reporte direta com os responsáveis pela governação.

9. Se, com base na compreensão preliminar do auditor sobre a função de auditoria interna, o auditor espera utilizar o trabalho da função de auditoria interna para modificar a natureza ou oportunidade, ou reduzir a extensão dos procedimentos de auditoria a executar, a ISA 610 (Revisão 2013) aplica-se.

10. Como é discutido em mais detalhe na ISA 610 (Revisão 2013), as atividades de uma função de auditoria interna são distintas de outros controlos de monitorização que podem ser relevantes para o relato financeiro, como revisões de informações contabilísticas de gestão que são concebidas para contribuir para a forma como a entidade previne ou deteta erros.

11. Estabelecer comunicações com os indivíduos adequados no âmbito da função de auditoria interna de uma entidade no início do compromisso, e manter tais comunicações ao longo deste, pode facilitar a partilha eficaz de informação. Cria um ambiente em que o auditor pode ser informado de questões significativas que podem vir a chamar a atenção da função de auditoria interna quando tais questões possam afetar o trabalho do auditor. A ISA 200 aborda a importância de o auditor planear e executar a auditoria com ceticismo profissional[75], incluindo estar atento a informações que possam pôr em causa a fiabilidade dos documentos e das respostas aos inquéritos a serem usados como prova de auditoria. Por conseguinte, a comunicação com a função de auditoria interna ao longo do compromisso pode proporcionar aos auditores internos oportunidades para chamar a atenção do auditor para essa informação. O auditor pode então ter em conta essas informações na identificação e avaliação do auditor dos riscos de distorção material.

[75] ISA 200, parágrafo 7

Apêndice 5

(Ref: Para. 25(a), 26(b)-(c), A94, A166-A172)

Considerações para a Compreensão das Tecnologias da informação (TI)

Este apêndice fornece questões adicionais que o auditor pode considerar para compreender a utilização das TI pela entidade no seu sistema de controlo interno.

Compreender a utilização, pela Entidade, das Tecnologias de Informação nas Componentes do Sistema de Controlo Interno da Entidade

1. O sistema de controlo interno de uma entidade contém elementos manuais e elementos automatizados (isto é, controlos manuais e automatizados e outros recursos utilizados no sistema de controlo interno da entidade). A mistura de elementos manuais e automatizados de uma entidade varia com a natureza e complexidade da utilização de TI por parte da entidade. A utilização de TI por parte de uma entidade afeta a forma como a informação relevante para a elaboração das demonstrações financeiras de acordo com a estrutura de relato financeiro aplicável é processada, armazenada e comunicada, afetando assim a forma como o sistema de controlo interno da entidade é concebido e implementado. Cada componente do sistema de controlo interno da entidade pode utilizar em alguma medida as TI.

   Geralmente, as TI beneficiam o sistema de controlo interno de uma entidade, permitindo a uma entidade:

   - Aplicar de forma consistente regras comerciais predefinidas e realizar cálculos complexos no processamento de grandes volumes de transações ou dados;
   - Melhorar a oportunidade, disponibilidade e precisão da informação;
   - Facilitar a análise adicional da informação;
   - Melhorar a capacidade de monitorizar o desempenho das atividades da entidade e as suas políticas e procedimentos;
   - Reduzir o risco de que os controlos serem contornados;
   - Aumentar a capacidade de alcançar uma segregação de funções eficaz através da implementação de controlos de segurança em aplicações de TI, bases de dados e sistemas operativos.

2. As características dos elementos manuais ou automatizados são relevantes para a identificação e avaliação do auditor dos riscos de distorção material e para os procedimentos de auditoria daí resultantes. Os controlos automatizados podem ser mais fiáveis do que os controlos manuais, porque não podem ser tão facilmente contornados, ignorados ou ultrapassados, e também são menos propensos a simples erros e enganos. Os controlos automatizados podem ser mais eficazes do que os controlos manuais nas seguintes circunstâncias:

   - Grande volume de transações recorrentes, ou em situações em que os erros que podem ser antecipados ou previstos podem ser prevenidos, ou detetados e corrigidos, através da automatização.
   - Controlos onde as formas específicas de executar o controlo podem ser adequadamente concebidas e automatizadas.

Compreender a utilização, por parte da Entidade, das Tecnologias da Informação no Sistema de Informação (Ref: Para. 25 (a))

3. O sistema de informação da entidade pode incluir a utilização de elementos manuais e automatizados, que também afetam a forma como as transações são iniciadas, registadas, processadas e relatadas. Em particular, os procedimentos para iniciar, registar, processar e relatar transações podem ser reforçados através das aplicações de TI utilizadas pela entidade e pela forma como a entidade configura essas aplicações. Além disso, os registos sob a forma de informação digital podem substituir ou complementar registos sob a forma de documentos em papel.

4. Ao obter uma compreensão do ambiente de TI relevante para os fluxos de transações e tratamento da informação no sistema de informação, o auditor reúne informações sobre a natureza e as características das aplicações informáticas utilizadas, bem como sobre a infraestrutura informática de apoio e sobre as TI. O quadro que se segue inclui exemplos de questões que o auditor pode considerar na obtenção da compreensão do ambiente de TI e inclui exemplos de características típicas de ambientes de TI baseados na complexidade das aplicações informáticas utilizadas no sistema de informação da entidade. No entanto, tais características são orientadoras e podem diferir em função da natureza das aplicações específicas de TI utilizadas por uma entidade.

	Exemplos de características típicas de:		
	Software comercial não complexo	Software comercial ou aplicações de TI de tamanho médio e moderadamente complexo	Aplicações de TI grandes ou complexas (por exemplo, sistemas ERP)
Questões relacionadas com a extensão da automatização e utilização de dados:			
• Extensão dos procedimentos automatizados de processamento e a complexidade desses procedimentos, incluindo, se se trata de um processamento altamente automatizado e sem papel.	N/A	N/A	Procedimentos automatizados extensivos e muitas vezes complexos
• Extensão da confiança da entidade em relatórios gerados pelo sistema no processamento de informação.	Lógica de relatório automatizado simples	Lógica de relatório automatizado relevante simples	Lógica de relatório automatizado complexo; Software de autoria de relatórios
• Forma como os dados são introduzidos (isto é, entrada manual, entrada efetuada por cliente ou fornecedor, ou carga de ficheiro).	Entrada de dados manual	Pequeno número de entradas de dados ou interfaces simples	Um grande número de entradas de dados ou interfaces complexos
• Forma como as TI facilitam a comunicação entre aplicações, bases de dados ou outros aspetos do ambiente de TI, interna e externamente, conforme adequado, através de interfaces do sistema.	Sem interfaces automatizados (apenas entradas manuais)	Pequeno número de entradas de dados ou interfaces simples	Grande número de entradas de dados ou interfaces complexos
• O volume e a complexidade dos dados em formato digital que estão a ser tratados pelo sistema de informação, incluindo se os registos contabilísticos ou outras informações são armazenados em formato digital e a localização dos	Baixo volume de dados ou dados simples que possam ser verificados manualmente; Dados disponíveis localmente	Baixo volume de dados ou dados simples	Grande volume de dados ou dados complexos; Armazéns de dados[76]; Utilização de prestadores de serviços de TI internos ou externos (por exemplo, armazenamento ou

[76] Um armazém de dados é geralmente descrito como um repositório central de dados integrados provenientes de uma ou mais fontes distintas (tais como várias bases de dados), a partir do qual podem ser gerados relatórios ou que pode ser utilizado pela entidade para outras atividades de análise de dados. Um gerador de relatórios é uma aplicação informática utilizada para extrair dados de uma ou mais fontes (tais como um armazém de dados, uma base de dados ou uma aplicação informática) e apresentar os dados num formato específico

	Exemplos de características típicas de:		
dados armazenados.			hospedagem de dados por terceiros)
Questões relacionadas com as aplicações de TI e infraestruturas de TI:			
• Tipo de aplicação (por exemplo, uma aplicação comercial com pouca ou nenhuma personalização, ou uma aplicação altamente personalizada ou altamente integrada que pode ter sido comprada e personalizada, ou desenvolvida internamente).	Aplicação comprada com pouca ou nenhuma personalização	Aplicação adquirida ou antigas simples ou aplicações ERP de gama baixa com pouca ou nenhuma personalização	Aplicações desenvolvidas personalizadas ou ERP mais complexos com personalização significativa
• Complexidade da natureza das aplicações de TI e a infraestrutura de TI subjacente.	Portáteis pequenos e simples ou soluções baseadas em server de clientes	Computador principal maduro e estável, servidor de clientes pequeno ou simples, nuvem como serviço de software	Computador principal complexo, servidor de clientes grande ou complexo, viradas para a web, nuvem como serviço de infraestrutura
• Se existe hospedagem por terceiros ou subcontratação de TI.	Se for subcontratado, fornecedor comprovadamente competente, maduro (por exemplo, fornecedor de nuvem)	Se for subcontratado, fornecedor comprovadamente competente e maduro (por exemplo, fornecedor de nuvem)	Prestador comprovadamente competente e maduro para determinadas aplicações e fornecedor novo ou de arranque para outras
• Se a entidade está a utilizar tecnologias emergentes que afetam o seu relato financeiro.	Não utilização de tecnologias emergentes	Utilização limitada de tecnologias emergentes em algumas aplicações	Uso misto de tecnologias emergentes transversalmente nas plataformas
Questões relacionadas com processos de TI:			
• Pessoal envolvido na manutenção do ambiente de TI (o número e o nível de competência dos recursos de suporte de TI que gerem a segurança e as alterações ao ambiente de TI).	Poucos funcionários com conhecimentos de TI limitados para processar atualizações de fornecedores e gerir acessos	Pessoal limitado com competências em TI / dedicado a TI	Departamentos de TI dedicados com pessoal qualificado, incluindo competências de programação
• A complexidade dos processos para gerir os direitos de acesso.	Indivíduo único com acesso administrativo	Poucas pessoas com acesso administrativo gerem direitos de acesso	Processos complexos geridos pelo

	Exemplos de características típicas de:		
	gere direitos de acesso		departamento de TI para direitos de acesso
• A complexidade da segurança sobre o ambiente informático, incluindo a vulnerabilidade das aplicações de TI, bases de dados e outros aspetos do ambiente informático para riscos cibernéticos, especialmente quando existem transações na Web ou transações que envolvem interfaces externas.	Acesso local simples sem elementos externos virados para a web	Algumas aplicações baseadas na web com segurança principalmente simples e baseada em funções	Múltiplas plataformas com acesso baseado na Web e modelos de segurança complexos
• Se foram feitas alterações no programa à maneira como a informação é processada e a extensão dessas alterações durante o período.	Software comercial sem código fonte instalado	Algumas aplicações comerciais sem código fonte e outras aplicações maduras com um pequeno número ou alterações simples; ciclo de vida de desenvolvimento de sistemas tradicionais	Novas ou um grande número ou alterações complexas, vários ciclos de desenvolvimento todos os anos
• A extensão da mudança no ambiente das TI (por exemplo, novos aspetos do ambiente de TI ou alterações significativas nas aplicações de TI ou na infraestrutura de TI subjacente).	Alterações limitadas a atualizações de versão de software comercial	As alterações consistem em atualizações de software comercial, atualizações de versão ERP ou melhorias a sistemas antigos	Novos ou um número grande ou mudanças complexas, vários ciclos de desenvolvimento todos os anos, personalização pesada de ERP
• Se houve uma grande conversão de dados durante o período e, em caso afirmativo, a natureza e o significado das alterações efetuadas e a forma como a conversão foi efetuada.	Atualizações de software fornecidas pelo fornecedor; Inexistência de funcionalidades de conversão de dados para atualizar	Pequenas atualizações de versões de aplicações de software comercial com dados limitados a serem convertidos	Grandes atualizações de versões, novo lançamento, mudança de plataforma

Tecnologias Emergentes

5. As entidades podem utilizar tecnologias emergentes (por exemplo, *blockchain*, robótica ou inteligência artificial) porque tais tecnologias podem apresentar oportunidades específicas para aumentar a eficiência operacional ou melhorar o relato financeiro. Quando as tecnologias emergentes forem utilizadas no sistema de informação da entidade relevante para a elaboração das demonstrações financeiras, o auditor pode incluir essas tecnologias na identificação de aplicações informáticas e outros aspetos do ambiente de TI que estão sujeitos a riscos decorrentes da utilização de TI. Embora as tecnologias emergentes possam ser consideradas mais sofisticadas ou mais complexas em comparação com as tecnologias existentes, as responsabilidades do auditor em relação às aplicações de TI e aos controlos gerais de TI identificados em conformidade com a alínea b do ponto 26(b)-(c) permanecem inalteradas.

Escalabilidade

6. Obter uma compreensão do ambiente de IT da entidade pode ser mais facilmente conseguido para uma entidade menos complexa que utiliza software comercial e quando a entidade não tem acesso ao código fonte para fazer quaisquer alterações ao programa. Estas entidades podem não ter recursos de TI dedicados, mas podem ter uma pessoa atribuída numa função de administrador com o objetivo de conceder acesso aos colaboradores ou instalar atualizações às aplicações de TI fornecidas pelo fornecedor. Questões específicas que o auditor pode considerar na compreensão da natureza de um pacote de software de contabilidade comercial, que pode ser a única aplicação de TI utilizada por uma entidade menos complexa no seu sistema de informação, podem incluir:

    - Até que ponto o software está bem estabelecido e tem uma reputação de fiabilidade;
    - A medida em que é possível à entidade modificar o código fonte do software para incluir módulos adicionais (isto é, *add-ons*) no *software* base ou para então fazer alterações diretas aos dados;
    - A natureza e extensão das modificações que foram feitas ao software. Embora uma entidade possa não ser capaz de modificar o código fonte do software, muitos pacotes de software permitem a configuração (por exemplo, definir ou alterar parâmetros de relatórios). Estes não envolvem geralmente modificações ao código fonte; todavia, o auditor pode considerar até que ponto a entidade pode configurar o software ao considerar a completude e a exatidão das informações produzidas pelo software que é utilizado como prova de auditoria; e
    - Até que ponto os dados relacionados com a preparação das demonstrações financeiras podem ser diretamente acedidos (isto é, acesso direto à base de dados sem utilização da aplicação de TI) e o volume de dados que são tratados. Quanto maior for o volume de dados, maior é a probabilidade de a entidade necessitar de controlos que abordem a manutenção da integridade dos dados, o que pode incluir controlos gerais de TI sobre acesso e alterações não autorizadas a dados.

7. Ambientes complexos de TI podem incluir aplicações de TI altamente personalizadas ou altamente integradas, podendo, portanto, exigir mais esforços para serem compreendidos. Os processos de reporte financeiro ou aplicações de TI podem ser integrados com outras aplicações de TI. Essa integração pode envolver aplicações informáticas utilizadas nas operações comerciais da entidade e que forneçam informações aos pedidos de TI relevantes para os fluxos de transações e tratamento da informação no sistema de informação da entidade. Nestas circunstâncias, certos pedidos de TI utilizados nas operações comerciais da entidade podem igualmente ser relevantes para a elaboração das demonstrações financeiras. Ambientes complexos de TI também podem exigir departamentos de TI dedicados que tenham processos estruturados de TI apoiados por pessoal que tenha competências no desenvolvimento de software e de manutenção do ambiente de TI. Noutros casos, uma entidade pode utilizar prestadores de serviços internos ou externos para gerir certos aspetos ou processos de TI no seu ambiente de TI (por exemplo, hospedagem por terceiros).

Identificar aplicações de TI sujeitas a riscos decorrentes da utilização de TI

8. Através da compreensão da natureza e complexidade do ambiente de TI da entidade, incluindo a natureza e extensão dos controlos de processamento de informação, o auditor pode determinar quais as aplicações de TI em que a entidade está a confiar para processar e manter com precisão a integridade das informações financeiras. A identificação dos pedidos de TI em que a entidade se baseia pode afetar a decisão do auditor de testar os controlos automatizados dentro desses pedidos de TI, assumindo que esses controlos automatizados abordam os riscos identificados de distorção material. Inversamente, se a entidade não estiver a confiar numa aplicação de TI, é pouco provável que os controlos automatizados no âmbito dessa aplicação de TI sejam adequados ou suficientemente precisos para efeitos de testes de eficácia operacional. Os controlos automatizados que possam ser identificados de acordo com o parágrafo 26 (b) podem incluir, por exemplo, cálculos automatizados ou controlos de entrada, processamento e saída, tais como uma correspondência a três de uma encomenda de compra, documento de envio do fornecedor e fatura do fornecedor. Quando os controlos automatizados são identificados pelo auditor e o auditor determina, através da compreensão do ambiente de TI, que a entidade confia na aplicação de TI que inclui esses controlos automatizados, pode ser mais provável que o auditor identifique a aplicação de TI como uma que está sujeita a riscos decorrentes da utilização de TI.

9. Ao analisar se as aplicações de TI para os quais o auditor identificou controlos automatizados estão sujeitos a riscos decorrentes da utilização de TI, o auditor é suscetível de analisar se, e em que medida, a entidade pode ter acesso ao código fonte que permite à administração efetuar alterações nos programas a esses controlos ou aplicações de TI. A medida em que a entidade faz alterações de programas ou de configurações e a medida em que os processos de TI sobre tais alterações são formalizados podem também ser considerações relevantes. Também é provável que o auditor considere o risco de acesso inadequado ou alterações aos dados.

10. Os relatórios gerados pelo sistema que o auditor pode pretender utilizar como prova de auditoria podem incluir, por exemplo, um relatório de antiguidade de saldos a receber ou um relatório de valorização do inventário. Para esses relatórios, o auditor pode obter provas de auditoria sobre a plenitude e exatidão dos relatórios, testando de forma substantiva os inputs e os resultados do relatório. Em outros casos, o auditor pode planear testar a eficácia operacional dos controlos sobre a preparação e manutenção do relatório, caso em que o pedido de TI a partir do qual é produzido é suscetível de estar sujeito a riscos decorrentes da utilização de TI. Além de testar a plenitude e a exatidão do relatório, o auditor pode planear testar a eficácia operacional dos controlos gerais de TI que abordam riscos relacionados com alterações de programa inadequadas ou não autorizadas ao relatório ou a alterações de dados neste.

11. Algumas aplicações de TI podem incluir a funcionalidade de escrita de relatórios dentro delas, enquanto algumas entidades podem também utilizar aplicações separadas de redação de relatórios (isto é, escritoras de relatórios). Nesses casos, o auditor poderá ter de determinar as fontes dos relatórios gerados pelo sistema (isto é, a aplicação que prepara o relatório e as fontes de dados utilizadas pelo relatório) para determinar os pedidos de TI sujeitos a riscos decorrentes da utilização de TI.

12. As fontes de dados utilizadas por aplicações de TI podem ser bases de dados que, por exemplo, só podem ser acedidas através da aplicação de TI ou por pessoal de TI com acessos de administração de bases de dados. Noutros casos, a fonte de dados pode ser um armazenamento de dados que pode só por si ser considerado como uma aplicação de TI sujeita a riscos decorrentes da utilização de TI.

13. O auditor pode ter identificado um risco para o qual os procedimentos substantivos por si só não são suficientes devido à utilização, por parte da entidade, de um tratamento de transações altamente automatizado e sem papel, o que pode implicar múltiplas aplicações de IT integradas. Nestas circunstâncias, é provável que os controlos identificados pelo auditor incluam controlos automatizados. Além disso, a entidade pode estar a contar com controlos gerais de TI para manter a integridade das transações processadas e de outras informações utilizadas no processamento. Nesses casos, as aplicações de TI envolvidas no tratamento e no armazenamento das informações estão, provavelmente, sujeitas a riscos decorrentes da utilização de TI.

Computação de Utilizador Final

14. Embora os elementos de prova de auditoria possam também vir sob a forma de uma saída gerada pelo sistema que é utilizada num cálculo realizado numa ferramenta de computação de utilizador final (por exemplo, software de folha de cálculo ou bases de dados simples), tais ferramentas não são tipicamente identificadas como aplicações de TI no contexto do parágrafo 26 (b). A conceção e implementação de controlos em torno do acesso e alteração das ferramentas de computação do utilizador final pode ser um desafio, e esses controlos raramente são equivalentes ou tão eficazes como os controlos gerais de TI. Em vez disso, o auditor pode considerar uma combinação de controlos de processamento de informação, tendo em conta o objetivo e a complexidade envolvida na computação do utilizador final, tais como:

    - Controlos de processamento de informação sobre o início e tratamento dos dados fonte, incluindo controlos automatizados ou de interface relevantes até ao ponto de onde os dados são extraídos (isto é, o armazém de dados);
    - Controlos para verificar que a lógica está a funcionar como pretendido, por exemplo, controlos que "comprovem" a extração de dados, tais como conciliar o relatório com os dados de onde este foi derivado, comparando os dados individuais do relatório com a fonte e vice-versa, e controlos que verificam as fórmulas ou macros; ou
    - Utilização de ferramentas de validação de software, que verificam sistematicamente fórmulas ou macros, tais como ferramentas de integridade da folhas de cálculo.

Escalabilidade

15. A capacidade da entidade para manter a integridade da informação armazenada e processada no sistema de informação pode variar em função da complexidade e volume das transações e outras informações relacionadas. Quanto maior for a complexidade e volume de dados que suporta uma classe de transações, saldo de conta ou divulgação significativas, menos provável se pode tornar a possibilidade de a entidade manter a integridade dessa informação apenas através de controlos de processamento de informação (por exemplo, controlos de entrada e saída ou controlos de revisão). Torna-se igualmente menos provável que o auditor possa obter provas de auditoria sobre a plenitude e exatidão dessas informações apenas através de testes substantivos quando essas informações forem utilizadas como prova de auditoria. Em algumas circunstâncias, quando o volume e a complexidade das transações forem menores, a gestão pode ter um controlo de processamento de informação suficiente para verificar a exatidão e a plenitude dos dados (por

exemplo, as ordens de encomendas de vendas individuais processadas e faturadas podem ser reconciliadas com a cópia em papel originalmente inserida na aplicação de TI). Quando a entidade se basear em controlos gerais de TI para manter a integridade de certas informações utilizadas por aplicações informáticas, o auditor pode considerar que as aplicações de TI que mantêm essa informação estão sujeitos a riscos decorrentes da utilização de TI.

Exemplos de características de uma aplicação de TI que provavelmente não está sujeita a riscos decorrentes de TI	Exemplos de características de uma aplicação de TI que está provavelmente sujeita a riscos decorrentes de TI
• Aplicações autónomas. • O volume de dados (transações) não é significativo. • A funcionalidade da aplicação não é complexa. • Cada transação é suportada por documentação original em cópia impressa.	• As aplicações são interligadas. • O volume de dados (transações) é significativo. • A funcionalidade da aplicação é complexa, uma vez que: ○ A aplicação inicia automaticamente as transações; e ○ Há uma variedade de cálculos complexos subjacentes às entradas automatizadas.
• A aplicação de TI não está provavelmente sujeita a riscos decorrentes de TI porque: • O volume de dados não é significativo e, por conseguinte, a gestão não depende dos controlos gerais de TI para processar ou manter os dados.	• A aplicação de TI está provavelmente sujeita a riscos decorrentes de TI porque: • A gestão baseia-se numa aplicação do sistema para processar ou manter dados, uma vez que o volume de dados é significativo.
• A gestão não depende de controlos automatizados ou de outras funcionalidades automatizadas. O auditor não identificou controlos automatizados em conformidade com o parágrafo 26 (a). • Embora a gestão utilize relatórios gerados pelo sistema nos seus controlos, não depende destes relatórios. Em vez disso, concilia os relatórios com a documentação impressa e verifica os cálculos dos relatórios. • O auditor irá testar diretamente as informações produzidas pela entidade utilizada como prova de auditoria.	• A gestão confia em aplicações do sistema para executar certos controlos automatizados que o auditor também identificou.

Outros Aspetos do Ambiente de TI que Estão Sujeitos a Riscos Decorrentes da utilização de TI

16. Quando o auditor identifica aplicações de TI que estão sujeitas a riscos decorrentes da utilização de TI, outros aspetos do ambiente de TI estão também tipicamente sujeitos a riscos decorrentes da utilização de TI. A infraestrutura de TI inclui as bases de dados, o sistema operativo e a rede. As bases de dados armazenam os dados utilizados pelas aplicações de TI e podem consistir em muitas tabelas de dados interligadas. Os dados em bases de dados também podem ser acedidos diretamente, através de sistemas de gestão de bases de dados, por pessoal TI ou outro com acessos de administração de bases de dados. O sistema operativo é responsável pela gestão de comunicações entre hardware, aplicações de TI e outros softwares utilizados na rede. Como tal, as aplicações e bases de dados de TI podem ser diretamente acedidas através do sistema operativo. Uma rede é utilizada na infraestrutura de TI para transmitir dados e para partilhar informações, recursos e serviços através de uma ligação comum de comunicações. A rede também estabelece, tipicamente, uma camada de segurança lógica (posta em prática através do sistema operativo) para o acesso aos recursos subjacentes.

17. Quando as aplicações de TI são identificadas pelo auditor como estando sujeitas a riscos decorrentes de TI, a(s) base(s) de dados que armazena(m) os dados tratados por uma aplicação de TI identificada, por norma também é(são) identificada(s). Da mesma forma, uma vez que a capacidade de funcionamento de uma aplicação de TI

depende frequentemente do sistema operativo e as aplicações e as bases de dados de TI podem ser diretamente acedidas a partir do sistema operativo, o sistema operativo está normalmente sujeito a riscos decorrentes da utilização de TI. A rede pode ser identificada quando se trata de um ponto central de acesso às aplicações de TI identificadas e às bases de dados conexas ou quando uma aplicação de TI interage com fornecedores ou partes externas através da internet, ou quando são identificadas pelo auditor aplicações de TI viradas para a Web.

Identificar riscos decorrentes da utilização de TI e controlos gerais de TI

18. Exemplos de riscos decorrentes da utilização de TI incluem riscos relacionados com a confiança inadequada em aplicações de TI que estão a efetuar processamentos incorretos de dados, a processar dados incorretos, ou ambos, tais como:

    - Acesso não autorizado a dados que pode resultar na destruição de dados ou em alterações impróprias de dados, incluindo o registo de transações não autorizadas ou inexistentes, ou o registo incorreto de transações. Podem surgir riscos específicos quando vários utilizadores acedem a uma base de dados comum.
    - A possibilidade de o pessoal de TI obter privilégios de acesso para além dos necessários para desempenhar as funções que lhe estão atribuídas, quebrando, assim, a segregação de funções.
    - Alterações não autorizadas aos dados nos ficheiros principais.
    - Alterações não autorizadas nas aplicações de TI ou em noutros aspetos do ambiente de TI.
    - Não serem feitas alterações necessárias às aplicações de TI ou a outros aspetos do ambiente de TI.
    - Intervenções manuais inadequadas.
    - Perda potencial de dados ou incapacidade de aceder aos dados conforme necessário.

19. A consideração do auditor sobre o acesso não autorizado pode incluir riscos relacionados com o acesso não autorizado por partes internas ou externas (muitas vezes referidos como riscos de cibersegurança). Tais riscos podem não afetar necessariamente o relato financeiro, uma vez que o ambiente de TI de uma entidade também pode incluir aplicações de TI e dados relacionados que respondem às necessidades operacionais ou de conformidade. É importante notar que os incidentes cibernéticos ocorrem geralmente primeiro através do perímetro e das camadas internas da rede, que tendem depois a ser removidas da aplicação de TI, da base de dados e dos sistemas operativos que afetam a preparação das demonstrações financeiras. Por conseguinte, se for identificada informação sobre uma violação de segurança, o auditor normalmente considera até que ponto essa violação tem o potencial de afetar o relato financeiro. Se o relato financeiro puder ser afetado, o auditor pode decidir compreender e testar os controlos conexos, para determinar o possível impacto ou o âmbito de eventuais distorções nas demonstrações financeiras, ou pode determinar que a entidade efetuou divulgações adequadas em relação a essa violação de segurança.

20. Adicionalmente, leis e regulamentos que possam ter um efeito direto ou indireto nas demonstrações financeiras da entidade podem incluir legislação de proteção de dados. Considerar o cumprimento de tais leis ou regulamentos por parte de uma entidade, de acordo com a ISA 250 (Revista), pode implicar a compreensão dos processos de TI da entidade e os controlos gerais de TI que a entidade implementou para abordar as leis ou regulamentos relevantes.

21. São implementados controlos gerais de TI para fazer face a riscos decorrentes da utilização de TI. Por conseguinte, o auditor utiliza o entendimento obtido sobre as aplicações de TI identificadas e outros aspetos do ambiente de TI e os riscos aplicáveis decorrentes da utilização de TI ao determinar os controlos gerais de TI a identificar. Em alguns casos, uma entidade pode utilizar processos comuns de TI transversais a todo o seu ambiente de TI ou transversais a certos aplicativos de TI, caso em que podem ser identificados riscos comuns decorrentes da utilização de TI e controlos gerais comuns de TI.

22. Em geral, é provável que seja identificado um número maior de controlos gerais de TI relacionados com aplicações e bases de dados de TI do que relacionados com outros aspetos do ambiente das TI. Isto porque estes aspetos são os mais estreitamente relacionados com o processamento e armazenamento de informação no sistema de informação da entidade. Ao identificar os controlos gerais de TI, o auditor pode considerar controlos sobre as ações tanto dos utilizadores finais como do pessoal de TI e dos prestadores de serviços de TI da entidade.

23. O **Apêndice 6** fornece uma explicação mais aprofundada da natureza dos controlos gerais de TI normalmente implementados para diferentes aspetos do ambiente de TI. Além disso, são fornecidos exemplos de controlos gerais de TI para diferentes processos de TI.

Apêndice 6

(Ref: Para. 26(c), A173-A174)

Considerações para a Compreensão dos Controlos Gerais de TI

Este apêndice fornece outras questões que o auditor pode considerar na compreensão dos controlos gerais das TI.

1. Natureza dos controlos gerais de TI normalmente implementados para cada um dos aspetos do ambiente de TI:

   (a) Aplicações

   Os controlos gerais de TI ao nível da aplicação de TI correlacionar-se-ão com a natureza e extensão da funcionalidade da aplicação e com os caminhos de acesso permitidos na tecnologia. Por exemplo, mais controlos serão relevantes para aplicações de TI altamente integradas com opções de segurança complexas do que para uma aplicação de TI antiga que suporta um pequeno número de saldos de conta com métodos de acesso apenas através de transações.

   (b) Base de dados

   Os controlos gerais de TI ao nível da base de dados normalmente abordam os riscos decorrentes da utilização de TI relacionados com atualizações não autorizadas a informações de relato financeiro na base de dados, através do acesso direto à base de dados ou da execução de um *script* ou programa.

   (c) Sistema Operativo

   Os controlos gerais de TI ao nível do sistema operativo normalmente abordam os riscos decorrentes da utilização de TI relacionados com o acesso administrativo, que podem facilitar a derrogação de outros controlos. Isto inclui ações como comprometer as credenciais de outros utilizadores, adicionar novos utilizadores não autorizados, carregar vírus informáticos ou executar scripts ou outros programas não autorizados.

   (d) Rede

   Os controlos gerais de TI ao nível da rede normalmente abordam os riscos decorrentes da utilização de TI relacionados com a segmentação da rede, acesso remoto e autenticação. Os controlos de rede podem ser relevantes quando uma entidade tem aplicações viradas para a Web utilizadas no relato financeiros. Os controlos de rede podem ser relevantes quando a entidade tem relações significativas com parceiros comerciais ou terceiros subcontratados, o que pode aumentar as transmissões de dados e a necessidade de acesso remoto.

2. Exemplos de controlos gerais de TI que podem existir, organizados por processo de TI incluem:

   (a) Processo de gestão do acesso:

   - *Autenticação*

     Os controlos que garantem que um utilizador que acede à aplicação de TI ou a outro aspeto do ambiente de TI está a utilizar as credenciais de login do próprio utilizador (ou seja, o utilizador não está a utilizar as credenciais de outro utilizador).

   - *Autorização*

     Controlos que permitem aos utilizadores aceder às informações necessárias para as suas responsabilidades no trabalho e nada mais, o que facilita a adequada segregação de funções.

   - *Atribuição*

     Controlos para autorizar novos utilizadores e modificações nos privilégios de acesso dos utilizadores existentes.

   - *Revogação*

     Controlos para remover o acesso do utilizador após rescisão ou transferência.

   - *Acesso privilegiado*

     Controlos sobre o acesso administrativo ou de utilizadores com mais poderes.

   - *Revisões dos acessos de utilizador*

Controlos para reconfirmar ou avaliar o acesso do utilizador para autorização contínua ao longo do tempo.

- *Configuração de controlos de segurança*

  Cada tecnologia geralmente tem configurações chave que ajudam a restringir o acesso ao ambiente.

- *Acesso físico*

  Controlos sobre o acesso físico ao centro de dados e ao hardware, uma vez que estes podem ser utilizados para anular outros controlos.

(b) Processo para gerir alterações ao programa ou outras alterações ao ambiente de TI:

- *Processo de gestão de alterações*

  Controlos sobre o processo de conceção, programação, teste e migração de alterações para um ambiente de produção (ou seja, utilizador final).

- *Segregação de funções sobre a migração das alterações*

  Controlos que segregam o acesso de fazer e migrar alterações para um ambiente de produção.

- *Desenvolvimento ou aquisição ou implementação de sistemas*

  Controlos sobre o desenvolvimento ou implementação inicial de aplicações de TI (ou em relação a outros aspetos do ambiente de TI).

- *Conversão de dados*

  Controlos sobre a conversão de dados durante o desenvolvimento, implementação ou atualizações do ambiente de TI.

(c) Processo de gestão de operações de TI

- *Calendarização de trabalhos*

  Controlos sobre o acesso a calendarizar e iniciar trabalhos ou programas que possam afetar o relato financeiro.

- *Monitorização de trabalhos*

  Controlos para monitorizar trabalhos ou programas de relato financeiro para execução com sucesso.

- *Cópias de segurança e recuperação*

  Os controlos para garantir que as cópias de segurança dos dados de relato financeiro ocorrem conforme planeado e que esses dados estão disponíveis e podem ser acedidos para uma recuperação atempada na eventualidade de uma interrupção ou ataque.

- *Deteção de intrusões*

  Controlos para monitorizar vulnerabilidades e ou intrusões no ambiente de TI.

O quadro a seguir ilustra exemplos de controlos gerais de TI para abordar exemplos de riscos decorrentes da utilização de TI, incluindo para diferentes aplicações de TI baseadas na sua natureza.

Processo	**Riscos**	**Controlos**	**Aplicações de TI**		
Processo de TI	**Exemplo Riscos Decorrentes da Utilização de TI**	**Exemplo Controlos Gerais de TI**	**Software comercial não complexo – Aplicável (sim/ não)**	**Software comercial ou aplicações de TI de média dimensão e complexidade moderada – Aplicável (sim/ não)**	**Aplicações de TI grandes ou complexas (por exemplo, sistemas ERP) – Aplicáveis (sim/ não)**
Gerir o Acesso		A gestão aprova a natureza e a	Sim – em vez da revisão de	Sim	Sim

Processo	**Riscos**	**Controlos**	**Aplicações de TI**		
Processo de TI	**Exemplo Riscos Decorrentes da Utilização de TI**	**Exemplo Controlos Gerais de TI**	**Software comercial não complexo – Aplicável (sim/ não)**	**Software comercial ou aplicações de TI de média dimensão e complexidade moderada – Aplicável (sim/ não)**	**Aplicações de TI grandes ou complexas (por exemplo, sistemas ERP) – Aplicáveis (sim/ não)**
	Privilégios de acesso de utilizador: Os utilizadores têm privilégios de acesso para além dos necessários para desempenhar os deveres que lhe estão atribuídos, o que pode criar uma inadequada segregação de funções.	extensão dos privilégios de acesso para novos utilizadores e modificação do acesso para utilizadores, incluindo a aplicação de perfis/funções padrão, operações críticas de relato financeiro e segregação de funções	acesso do utilizador mencionada abaixo		
		O acesso de utilizadores que cessaram emprego ou foram transferidos é removido ou modificado em tempo útil	Sim – em vez da revisão de acesso do utilizador mencionada abaixo	Sim	Sim
		O acesso do utilizador é revisto periodicamente	Sim – em vez de controlos de Acesso/Revogação acima	Sim - para certas aplicações	Sim
		A segregação de funções é monitorizada e os acessos conflituantes são removidos ou mapeado para os controlos atenuantes, que são documentados e testados	N/A – nenhum sistema permitiu a segregação	Sim - para certas aplicações	Sim
		Acesso privilegiado (por exemplo, configuração e administradores de dados e de	Sim – provavelmente apenas a nível da aplicação de TI	Sim – a nível da aplicação de TI e de certos níveis do ambiente de TI para a plataforma	Sim – em todas os níveis de ambiente de TI para plataforma

Processo	**Riscos**	**Controlos**	**Aplicações de TI**		
Processo de TI	**Exemplo Riscos Decorrentes da Utilização de TI**	**Exemplo Controlos Gerais de TI**	**Software comercial não complexo – Aplicável (sim/ não)**	**Software comercial ou aplicações de TI de média dimensão e complexidade moderada – Aplicável (sim/ não)**	**Aplicações de TI grandes ou complexas (por exemplo, sistemas ERP) – Aplicáveis (sim/ não)**
		segurança) é autorizado e devidamente restringido			
Gerir o Acesso	Acesso direto aos dados: Alterações inadequadas são feitas diretamente aos dados financeiros através de outros meios que não as transações das aplicações.	O acesso a ficheiros de dados de aplicações ou objetos/tabelas//dados de base de dados está limitado a pessoal autorizado, com base nas suas responsabilidades de trabalho e funções atribuídas, e esse acesso é aprovado pela administração	N/A	Sim - para determinadas aplicações e bases de dados	Sim
Gerir o Acesso	Definições do sistema: Os sistemas não estão configurados ou atualizados adequadamente para restringir o acesso do sistema a utilizadores devidamente autorizados e adequados.	O acesso é autenticado através de números de identificação e senhas de utilizador únicos ou outros métodos como um mecanismo para validar que os utilizadores estão autorizados a ter acesso ao sistema. Os parâmetros de palavra-passe cumprem os padrões da empresa ou do setor (por exemplo, comprimento mínimo da palavra-passe e complexidade, expiração, bloqueio de conta)	Sim – autenticação apenas com palavra-passe	Sim – mistura de palavra-passe e autenticação multi-fator	Sim
		Os atributos chave da configuração de	N/A – não existem	Sim - para determinadas	Sim

Processo	**Riscos**	**Controlos**	**Aplicações de TI**		
Processo de TI	**Exemplo Riscos Decorrentes da Utilização de TI**	**Exemplo Controlos Gerais de TI**	**Software comercial não complexo – Aplicável (sim/ não)**	**Software comercial ou aplicações de TI de média dimensão e complexidade moderada – Aplicável (sim/ não)**	**Aplicações de TI grandes ou complexas (por exemplo, sistemas ERP) – Aplicáveis (sim/ não)**
		segurança são devidamente implementados	configurações técnicas de segurança	aplicações e bases de dados	
Gerir a Mudança	Alterações de aplicação: São feitas alterações inadequadas a sistemas de aplicações ou programas que contêm controlos automatizados relevantes (isto é, parâmetros configuráveis, algoritmos automatizados, cálculos automatizados e extração automatizada de dados) ou lógica de relato.	Alterações a aplicações são devidamente testadas e aprovadas antes de serem transferidas para o ambiente de produção	N/A – deverá verificar-se que nenhum código fonte está instalado	Sim - para software não comercial	Sim
		O acesso à implementação de alterações no ambiente de produção das aplicações é adequadamente restringido e segregado do ambiente de desenvolvimento	N/A	Sim para software não comercial	Sim
Gerir a Mudança	Alterações na base de dados: São feitas alterações inadequadas à estrutura da base de dados e às relações entre os dados.	Alterações a base de dados são devidamente testadas e aprovadas antes de serem transferidas para o ambiente de produção	N/A – nenhuma alteração a bases de dados feita na entidade	Sim - para software não comercial	Sim
Gerir a Mudança	Alterações no software do sistema: São feitas alterações inadequadas ao software do sistema (por exemplo, sistema operativo, rede, software de gestão de alterações, software de	As alterações no software do sistema são devidamente testadas e aprovadas antes de serem transferidas para produção	N/A – não são feitas alterações no software do sistema na entidade	Sim	Sim

Processo	**Riscos**	**Controlos**	**Aplicações de TI**		
Processo de TI	**Exemplo Riscos Decorrentes da Utilização de TI**	**Exemplo Controlos Gerais de TI**	**Software comercial não complexo – Aplicável (sim/ não)**	**Software comercial ou aplicações de TI de média dimensão e complexidade moderada – Aplicável (sim/ não)**	**Aplicações de TI grandes ou complexas (por exemplo, sistemas ERP) – Aplicáveis (sim/ não)**
	controlo de acesso).				
Gerir a Mudança	Conversão de dados: Os dados convertidos de sistemas antigos ou versões anteriores geram erros de dados se a conversão transfere dados incompletos, redundantes, obsoletos ou imprecisos.	A gestão aprova os resultados da conversão de dados (por exemplo, atividades de balanceamento e reconciliação) das antigas aplicações de sistema ou da estrutura de dados para a nova aplicação do sistema ou estrutura de dados e monitoriza que a conversão é realizada de acordo com as políticas e procedimentos de conversão estabelecidos	N/A – Endereçado através de controlos manuais	Sim	Sim
Operações de TI	Rede: A rede não impede adequadamente os utilizadores não autorizados de terem acesso inadequado aos sistemas de informação.	O acesso é autenticado através de números de identificação únicos de utilizador e palavras-chave ou outros métodos como um mecanismo para validar que os utilizadores estão autorizados a ter acesso ao sistema. Os parâmetros de palavra-passe satisfazem as políticas e padrões da empresa ou profissionais (por exemplo, comprimento mínimo de palavra-passe e complexidade,	N/A – não existe nenhum método de autenticação de rede separado	Sim	Sim

Processo	**Riscos**	**Controlos**	**Aplicações de TI**		
Processo de TI	**Exemplo Riscos Decorrentes da Utilização de TI**	**Exemplo Controlos Gerais de TI**	**Software comercial não complexo – Aplicável (sim/ não)**	**Software comercial ou aplicações de TI de média dimensão e complexidade moderada – Aplicável (sim/ não)**	**Aplicações de TI grandes ou complexas (por exemplo, sistemas ERP) – Aplicáveis (sim/ não)**
		expiração, bloqueio de conta)			
		A rede é arquitetada para segmentar aplicações viradas web a partir da rede interna, onde as aplicações relevantes do controlo interno sobre o relato financeiro (ICFR) são acedidas	N/A – nenhuma segmentação de rede é usada	Sim - com julgamento	Sim - julgamento
		Numa base periódica, as análises de vulnerabilidade do perímetro da rede são realizadas pela equipa de gestão da rede, que também investiga potenciais vulnerabilidades	N/A	Sim - com julgamento	Sim - com julgamento
		Numa base periódica, são gerados alertas para fornecer notificação de ameaças identificadas pelos sistemas de deteção de intrusões. Estas ameaças são investigadas pela equipa de gestão de rede	N/A	Sim - com julgamento	Sim - com julgamento
		Controlos são implementados para restringir o acesso à Rede Privada Virtual (RPV) a utilizadores	N/A – sem RPV	Sim - com julgamento	Sim - com julgamento

Processo	**Riscos**	**Controlos**	**Aplicações de TI**		
Processo de TI	**Exemplo Riscos Decorrentes da Utilização de TI**	**Exemplo Controlos Gerais de TI**	**Software comercial não complexo – Aplicável (sim/ não)**	**Software comercial ou aplicações de TI de média dimensão e complexidade moderada – Aplicável (sim/ não)**	**Aplicações de TI grandes ou complexas (por exemplo, sistemas ERP) – Aplicáveis (sim/ não)**
		autorizados e apropriados			
Operações de TI	Cópias de segurança e recuperação dados:: Os dados financeiros não podem ser recuperados ou acedidos em tempo útil quando há perda de dados.	Os dados financeiros são sujeitos a cópias de segurança numa base regular de acordo com um calendário e frequência estabelecidos	N/A – confiança em cópias de segurança manuais da equipa financeira	Sim	Sim
Operações de TI	Calendarização de trabalhos: Sistemas de produção, programas ou trabalhos resultam num processamento impreciso, incompleto ou não autorizado de dados.	Apenas os utilizadores autorizados têm acesso à atualização dos trabalhos em lotes (incluindo trabalhos de interface) no software de calendarização de trabalhos	N/A – sem trabalhos em lotes	Sim - para certas aplicações	Sim
		Sistemas críticos, programas ou trabalhos são monitorizados, e os erros de processamento são corrigidos para assegurar a conclusão com sucesso.	N/A – sem monitorização de trabalhos	Sim - para certas aplicações	Sim