POLITÉCNICO
DO PORTO

AUDITORIA CONTÍNUA:

UM NOVO PARADIGMA DE AUDITORIA

Fernando Teixeira Pinto

Abril de 2011

NOTA PRÉVIA

O trabalho que se apresenta seguidamente visa dar resposta ao previsto no despacho Nº 12486/2010, de 16/7/2010 do Instituto Politécnico do Porto - atribuição do título de "especialista" no IPP.

Dada a recente publicação deste diploma e a falta de experiência da realização de trabalhos deste tipo, tentámos esclarecer junto do IPP o efectivo conteúdo que este trabalho deveria revestir, o que se revelou infrutífero.

Assim sendo, e dada a área de interesse que pretendemos tratar – a auditoria –, optámos por abordar uma área da auditoria que fosse inovadora e não as áreas tradicionais, a que, aliás, o autor tem estado ligado profissionalmente – a auditoria externa (ou financeira) e a auditoria interna.

Daí que se tenha optado por abordar uma área da auditoria que, sendo certamente incipiente em Portugal, suscita grande interesse e investigação na actualidade a nível internacional, quer de profissionais quer de académicos - a *auditoria contínua*.

ÍNDICE

Pág.

RESUMO

O ambiente de mudança e de incerteza, as novas tecnologias de informação subjacentes aos actuais sistemas de informação, a desmaterialização dos documentos, a produção de informação financeira on-line em tempo real, o comércio electrónico e os escândalos financeiros (sobretudo a partir do início dos anos 2000) – tudo isto colocou em causa o modelo tradicional de auditoria.

A auditoria contínua surge, há cerca de duas décadas, como um novo paradigma de auditoria susceptível de dar resposta às novas necessidades e ao novo contexto. É, pois, um tema recente, actualmente objecto de grande investigação e interesse, quer da parte de académicos quer de profissionais.

O presente trabalho aborda as principais inovações da auditoria contínua, os seus métodos e processos específicos, concluindo que a auditoria irá caminhar certamente no sentido deste novo paradigma, apesar dos obstáculos e dificuldades que uma mudança de tal dimensão enfrentará, exigindo alterações substanciais ao nível da regulação da profissão e do estatuto do auditor.

PALAVRAS-CHAVE

Auditoria contínua, auditoria tradicional, sistemas de informação, tecnologias de informação e comunicação, auditoria interna, controlo interno, gestão de riscos, governação, tempo real.

ABREVIATURAS

AICPA – American Institute of Certified Public Accountants

CICA – Canadian Institute of Chartered Accountants

COBIT – Control Objectives for Information and related Technologies

COSO – Committee of Sponsoring Organisations

ERP – Entreprise resource planning

IIA – Institute of Internal Auditors

ISACA – Information Systems Audit and Control Association

OROC – Ordem dos Revisores Oficiais de Contas

SI – sistemas de informação

SoX – Sarbanes-Oxley Act

TAAC (CAAT em inglês) - técnicas de auditoria assistidas por computador

TIC – Tecnologias de informação e comunicação

CAPÍTULO 1- INTRODUÇÃO

Diversos e conceituados autores confluem na afirmação de que o modelo tradicional de auditoria – baseado essencialmente em análises pontuais e descontínuas – se revela cada vez mais insuficiente e inadequado face às actuais circunstâncias.

A crise financeira de 2007/2008, os seus efeitos devastadores de diversa ordem – económicos, financeiros e sociais –, bem como alguns eventos financeiros escandalosos ocorridos desde o início dos anos 2000, contribuíram também poderosamente para que o paradigma tradicional da auditoria tenha vindo a ser questionado. Assim, tudo aponta para que, num futuro mais ou menos próximo, surja um novo paradigma de auditoria, como procuraremos demonstrar ao longo do presente trabalho.

Neste contexto, as tecnologias de informação e comunicação assumem hoje um papel crítico, porque os processos de negócio das entidades recorrem cada vez mais às TIC e estas têm-se vindo a tornar mais sofisticadas e complexas. Em termos de auditoria, as TIC introduzem novos factores de risco, mas um novo modelo de auditoria deve encará-las não nessa perspectiva, mas como uma efectiva oportunidade, como uma ferramenta de suporte à realização de um novo paradigma de auditoria – a auditoria contínua - capaz de potenciar e melhorar o controlo interno em benefício de todos os *stakeholders* de uma entidade.

Importa salientar que, com a introdução do computador nas empresas[1], a auditoria tornou-se em grande medida uma auditoria dos sistemas de informação organizacionais. No entanto, os objectivos da auditoria permanecem iguais, o que muda são os

[1] O primeiro computador empresarial remonta a 1954.

procedimentos e os métodos de que a auditoria se deve servir para se adaptar a este novo contexto.

A relação entre a auditoria e o computador pode considerar-se em diversas ópticas, que se sucederam historicamente:

- Auditoria *"à volta do"* computador: encarado como uma "caixa negra";
- Auditoria *"através do"* computador: a auditoria utiliza o computador na realização das suas actividades e procedimentos (aplicando as TAAC: técnicas de auditoria assistidas por computador);
- Auditoria *"com o"* computador: nesta fase mais avançada, o computador apoia, serve a auditoria.

A auditoria contínua e em tempo real que pretendemos estudar neste trabalho integra-se nesta última fase. O prazo de detecção de eventuais não conformidades é substancialmente encurtado, tornando-se a auditoria um factor de prevenção e de dissuasão.

A auditoria tem de se adaptar ao seu ambiente, às novas condições e às novas tecnologias, cujas potencialidades a auditoria poderá e deverá aproveitar em prol do seu próprio desenvolvimento. Na realidade, trata-se de adaptar o modelo da auditoria à era do digital e do electrónico, quando porventura o modelo ainda prevalecente é uma herança da era do papel. Num mundo caracterizado pela mudança, pela incerteza e pelo ritmo vertiginoso a que os eventos ocorrem, é manifesta a contradição entre o ritmo contínuo do ambiente informacional que se exprime em Mhz [2] e o ritmo do ser humano

[2] Mhz: abreviatura de megahertz – representa 1 milhão de hertz ou ciclos por segundo; medida usada para medir a velocidade das cpu's dos computadores.

que trabalha apenas 8h a 10h por dia. Esta discrepância coloca a questão da disponibilidade da informação em tempo útil, exacta, sob controlo adequado e objecto de um serviço de garantia do auditor prestado a idêntico ritmo.

Os novos sistemas de informação e as TIC afectam a auditoria essencialmente dos seguintes modos – através de dados processados sob forma electrónica (e já não sob a forma de papel), através do comércio electrónico (a realização de transacções on-line comporta factores de risco inerente específicos relevantes) e a publicação de informação financeira via Internet. Perante estas novas especificidades, a auditoria tem de adaptar o seu paradigma – e a auditoria contínua, objecto do presente trabalho, assume-se como uma via altamente adequada e promissora, como pretendemos investigar.

Há autores que radicam o imperativo da implementação da auditoria contínua na própria base regulamentar, mais especificamente no Sarbanes-Oxley Act dos Estados Unidos, na sua secção 409:

"Cada emitente que reporte sob a secção 13 ou 15 deve divulgar ao público numa base rápida e corrente qualquer informação adicional a respeito de alterações materiais na condição financeira ou operações do emitente, em inglês simples, que pode incluir informação qualitativa e tendencial e apresentações gráficas, como a Comissão determina, em regra, se necessário ou útil para a protecção dos investidores e no interesse público".

Os referidos autores entendem que o devido sentido deste texto regulamentar, em conjunto com as determinantes tecnológicas, torna a auditoria contínua inevitável a

prazo[3]. Relatos financeiros anuais ou trimestrais (e auditorias com idêntica periodicidade) revelam-se completamente desajustados dos tempos actuais.

A conjugação de ERP's integrados, de linguagens standard para informação financeira (como o XBRL) e a Internet criam as condições propícias para tal, como desenvolveremos.

O presente trabalho investiga o conteúdo do que se vem designando por auditoria contínua, as suas especificidades, os seus campos de aplicação mais promissores e adequados.

[3] Alles *et al.* (2004)

CAPÍTULO 2 - O CONCEITO

O conceito "auditoria contínua" foi introduzido pela primeira vez por Groomer e Murphy (em 1989) e Vasarhelyi e Halper (em 1991) [4].

No momento actual, não podemos falar correctamente em um só conceito, mas com mais rigor em vários conceitos de auditoria contínua.

No relatório de 1999 designado *Continuous Auditing*, elaborado por um grupo de trabalho da CICA e da AICPA, define-se auditoria contínua da seguinte forma – "uma metodologia que permite a auditores independentes (quer internos quer externos) fornecer garantia escrita sobre um dado assunto, usando uma série de relatórios de auditores emitidos simultaneamente ou após um curto período de tempo, da ocorrência dos eventos subjacentes ao assunto"

Rezaee *et al.* (2002), pelo seu lado, definem auditoria contínua como "processo de auditoria electrónico e compreensivo que permite aos auditores fornecer algum grau de garantia sobre a informação contínua simultaneamente com, ou pouco tempo após, a divulgação da informação".

Rezaee *et al.* (2001) apresentam ainda a seguinte definição de auditoria contínua - "um processo sistemático de juntar evidência electrónica de auditoria como uma base razoável para emitir uma opinião sobre a apresentação apropriada de demonstrações financeiras preparadas sob um sistema sem papel e em tempo real".

Para Helms e Mancino (1996), "auditoria contínua significou historicamente o uso de software para detectar excepções definidas pelo auditor de entre todas as transacções que são processadas quer em tempo real ou quase em tempo real. Estas excepções podem ser investigadas imediatamente ou escrita para um "log" de um auditor para trabalho subsequente",

Moeller (2009) define auditoria contínua [5] como "o processo de instalar *monitores* de controlo nos sistemas de tecnologia de informação de modo que tais monitores enviem sinais ou mensagens aos auditores – em regra auditores internos – se o processamento

[4] Citados por Chan, DY e Vasarhelyi, MA (2011)
[5] O autor chama-lhe "continuous assurance auditing"

do sistema assinala um desvio em relação a um limite ou a um parâmetro de auditoria". Nota-se aqui a ligação de auditoria contínua à auditoria interna.

Zhao et all (2004) apresenta o seguinte quadro comparativo entre a auditoria tradicional e a auditoria contínua:

	Auditoria tradicional	Auditoria contínua
Similitudes	> Certificação por auditores independentes	> Certificação por auditores independentes
	> Princípios contabilísticos geralmente aceites	> Princípios contabilísticos geralmente aceites
Diferenças	> Sistema de informação conta-bilístico baseado em papel	> Sistema de informação conta-bilístico sem papel
	> 1 vez por ano	> A pedido ou persistente

Já Santos (2009) afirma que "o modelo conceptual proposto (…) é de enorme relevância para as organizações, fornecendo um suporte de rigor e coerência, evitando a componente de subjectivismo que hoje é frequentemente aceite estar associada à realização de qualquer tipo de auditoria. A situação actual em que um mesmo processo organizacional é várias vezes auditado durante o ano para fins diversos (e.g. auditoria de qualidade, auditoria ambiental, auditoria financeira, auditoria operacional, auditoria de segurança) implica elevados custos e uma grande dispersão de recursos. Assim, a integração preconizada pelo modelo proposto pode ainda ser um factor de optimização de recursos".

Em termos académicos, a Universidade de Rutgers, em Newark, New Jersey, nos Estados Unidos, é considerada o mais avançado centro de investigação em auditoria contínua do mundo [6], contando com um conjunto de investigadores consagrados internacionalmente na matéria.

A análise das diversas definições de auditoria contínua apresentadas anteriormente permite-nos concluir que a expressão "auditoria contínua", como teremos oportunidade

[6] http://raw.rutgers.edu/continuousauditing

de desenvolver ao longo do presente trabalho, não reúne ainda um consenso, podendo dizer-se que tal expressão envolve conteúdos diferenciados:

- "Auditoria contínua" aplicada ao processo emergente de relato financeiro electrónico e em tempo real;

- "Auditoria contínua" aplicada à auditoria interna;

- "Auditoria contínua" numa perspectiva ampla e integrada dos diversos tipos de auditoria.

Passamos a desenvolver cada um destes entendimentos de "auditoria contínua".

I. Auditoria contínua e informação financeira *on-line*

O desenvolvimento tecnológico e a Internet em particular permitem a emissão de relato financeiro em tempo real às empresas (à medida que se efectuam as suas transacções, muitas delas também via Internet), o que determina a adaptação da auditoria financeira a este novo método de informação financeira, ou seja, a auditoria passa a ter de se pronunciar também (quase) em tempo real para ser efectiva.

A evidência visível tradicional desaparece e passa a assumir apenas forma electrónica. A auditoria tem de adaptar-se a este novo ambiente, deixando de ser baseada em papéis, adoptando um novo processo e modelo – electrónico, baseado em computador e contínuo.

Têm vindo a ser desenvolvidos standards preciosos para ajudar nesta tarefa, destacando-se o XBRL[7]. O XBRL é uma linguagem electrónica standardizada que permite extrair informação financeira dos diversos formatos.

A primeira versão do XBRL foi emitida em Julho de 2000, na sequência dum trabalho liderado pela AICPA, envolvendo diversas organizações profissionais, entre as quais as principais empresas de auditoria internacionais. A primeira chamada taxinomia [8] foi publicada em 31 de Julho de 2000 sob a título *"Financial Reporting for commercial and industrial companies under US GAAP".*

Com base no formato XBRL a informação financeira é introduzida apenas uma vez e depois pode ser convertida para diversas outras formas (impressão, HTML, EDGAR, etc.). O XBRL visa criar, portanto, uma linguagem standard entre empresas, auditores, Estado, etc. , conferindo fiabilidade a essa conversão.

Claro que as empresas que publicam informação financeira *on-line* em tempo real são ainda em número reduzido, como a Cisco Systems que afirma precisar de algumas horas para ter a informação actualizada.

[7] Baseado num sistema de etiquetagem Web chamado XML (eXtensible Markup Language).

[8] Deve entender-se por "taxinomias" dicionários de dados das contas necessários para preparar um conjunto de demonstrações financeiras com etiquetas XML de acordo com certos standards.

II. Auditoria contínua e auditoria interna

É certamente sob este entendimento – aplicação da filosofia de auditoria contínua à auditoria interna - que se encontra mais generalizadamente difundido o conceito de "auditoria contínua" e se encontram mais estudos e obras publicadas.

Relembremos o conceito fundamental de auditoria interna do IIA:

- "auditoria interna é uma actividade independente, de garantia e de consultoria, destinada a acrescentar valor e a melhorar as operações de uma organização. Ajuda a organização a alcançar os seus objectivos, através de uma abordagem sistemática e disciplinada, na avaliação e melhoria da eficácia dos processos de gestão de risco, de controlo e de governação".

Os sistemas de informação e as TIC cada vez mais sofisticadas e complexas afectaram imenso a auditoria interna tal como era tradicionalmente encarada, sobretudo por duas vias – através de dados processados sob forma electrónica (e não sob a forma de papel, perdendo-se a ancestral "evidência visível") e através do comércio electrónico (a realização de transacções on-line comporta factores de risco inerente tais como transacções não autorizadas ou distorções materiais).

Assiste-se a uma importância crescente da auditoria interna nas organizações mais relevantes, sendo chamada das tradicionais funções de avaliação do sistema de controlo interno – que continua certamente a ser a sua principal incumbência – para outras áreas como a gestão de risco, o governo das sociedades e serviços de consultoria. Por outro lado, a auditoria interna é requerida cada vez mais para ser um factor de criação de valor a favor das organizações.

Rezaee *et al.* (2001) afirmam que "o conhecimento do auditor interno do desenvolvimento da tecnologia de informação e do software de auditoria integrada tem de evoluir para assegurar auditoria *contínua* fornecendo credibilidade à informação financeira".

Os auditores internos são cada vez mais requeridos para dar apoio à gestão, sendo a auditoria episódica ou uma vez por ano insuficiente para as actuais circunstâncias e ambiente. Se acrescentarmos a luta contra a fraude e condutas indevidas e o constante

aperfeiçoamento das regras de *corporate governance*, a auditoria contínua parece ser a solução adequada para estas novas necessidades.

III. Auditoria contínua e integrada

Alguns autores como Santos (2009) sugerem mesmo um tipo de auditoria contínua que, na nossa opinião, deverá ser encarado como uma meta a alcançar a mais longo prazo por esta disciplina.

Na verdade, as empresas estão hoje em dia sujeitas a diversos tipos de auditoria com finalidades diversas – financeira, interna, de qualidade, ambiental, operacional ou de gestão, de segurança, entre outras – o que leva a que o mesmo processo organizacional seja auditado por diversas vezes, com o correspondente acréscimo significativo de custos.

É, pois, concebível uma auditoria contínua com esta abrangência, numa óptica de optimização e racionalização de recursos através de um modelo de auditoria contínua (on-line e em tempo real) e integrada (abarcando os diversos tipos de auditoria a que uma mesma entidade está sujeita). Temos aqui a auditoria contínua a contribuir não apenas para a tarefa tradicional de monitorização, mas também a contribuir para a eficiência de uma entidade.

Quando se fala em auditoria contínua e se analisa a questão da sua eficiência, importa colocar a questão da integração das diversas auditorias acima enumeradas a que uma entidade está hoje habitualmente sujeita no mesmo período de tempo. O modelo conceptual de auditoria deverá certamente acolher esta problemática e promover, tanto quanto possível, a integração dos diversos tipos de auditoria a que um mesmo processo organizacional pode estar sujeito. O mesmo processo seria auditado simultaneamente para as diversas perspectivas, em tempo real e on-line.

Uma auditoria deste tipo, a alcançar-se, seria uma auditoria holística e uma autêntica auditoria organizacional.

CAPÍTULO 3 - O PROCESSO

O processo tradicional de auditoria é afectado pela natureza específica da auditoria contínua em diversos pontos.

Na auditoria contínua, assiste-se a uma redução dos testes substantivos em favor de maior atenção depositada no sistema de controlo interno - na sua avaliação e eficácia -, colocando-se maior ênfase no risco inerente e no risco de controlo. Os testes aos controlos são cada vez mais testes electrónicos (exemplos: *firewalls*, passwords, encriptação da informação crítica).

Na auditoria tradicional, os testes aos controlos antecedem os testes substantivos, determinando a natureza, extensão e calendário destes últimos; na auditoria contínua, os testes aos controlos e os testes substantivos têm lugar em simultâneo.

O conhecimento do negócio e do sector de actividade da empresa merecem também um cuidado especial da parte do auditor para melhor identificação dos potenciais riscos, quando actuamos em auditoria contínua. O uso de demonstrações financeiras em tempo real em formato XBRL potencia o conhecimento do negócio e dos processos.

Na auditoria contínua, há lugar a uma utilização bastante mais intensa de TAAC [9] para avaliar riscos, avaliar controlos internos ou executar procedimentos de auditoria. Extracção de dados, contagem de registos, obtenção de dados por procedimentos analíticos, selecção de amostras (para testes aos controlos ou para testes substantivos), detecção de "excepções", detecção de transacções não usuais e confirmações são alguns exemplos de procedimentos de auditoria a executar por recurso a TAAC.

A auditoria contínua permite ao auditor testar 100% das populações objecto de análise, esbatendo a tradição do recurso à amostragem das transacções, tão habitual na auditoria financeira.

Os testes substantivos passam a ser executados ao longo do ano numa base *"ongoing"*, reduzindo-se a concentração dos mesmos em final de exercício.

[9] Ou CATT's em inglês: técnicas de auditoria assistidas por computador

Assiste-se a uma alteração da filosofia tradicional da auditoria de "olhar para o passado" - *"backword looking"* - para uma filosofia de auditoria contínua do sistema contabilístico e do sistema de controlo interno muito mais em cima dos factos.

Interessa realçar sobretudo o foco que a auditoria contínua faz incidir em dois aspectos:

- O sistema de controlo interno da entidade auditada
- O conhecimento do negócio da entidade auditada

No quadro seguinte sintetizamos as principais diferenças quanto ao processo de auditoria.

Processo de auditoria		
	Aud. Tradicional	Aud. Contínua
Testes substantivos	Maior utilização	Utilização mais reduzida
Testes substantivos	pontuais (final ano ou próximo)	regulares ("on-going")
Controlo interno	menor atenção do auditor	mais importantes e mais analisados pelo auditor
Conhecimento do negócio	menos importante	mais importante e analisado (gestão de risco)
TAAC	podem ser menos utilizadas	mais importantes e utilizadas
Amostragem	habitual	possibilidade testar 100%

Figura 1 – elaborado pelo autor

Algumas das diferenças referidas são de grande relevância, nomeadamente:

- A ênfase colocada pela auditoria contínua sobre a avaliação do sistema de controlo interno, em detrimento dos testes substantivos pontual e concentradamente executados, tantas vezes, na auditoria tradicional;

- A importância acrescida colocada no conhecimento do negócio;

- O menor recurso à amostragem, dado que a utilização de meios informáticos potentes permite analisar e testar a população integralmente.

Em auditoria contínua, são utilizadas frequentemente técnicas tais como: análise digital, *data mining*, etc. – para detectar factos e transacções não usuais.

CAPÍTULO 4 - A METODOLOGIA

A auditoria contínua exige a disponibilidade de uma infra-estrutura tecnológica que permita aceder e retirar dados de diversos tipos de ficheiros e registar formatos de diferentes sistemas e plataformas.

A normalização de dados é a maior dificuldade e desafio que se depara ao funcionamento de uma auditoria contínua.

O grau de automatismo em auditoria contínua depende de vários factores:

- Para ser elevado, exige que os módulos de auditoria estejam embebidos ou incorporados nos programas fonte (claro que esta integração tem custos que poderão ser significativos na fase inicial);
- Sendo menos automático, o auditor tem de tomar a iniciativa de fazer correr *"queries"* para detectar as excepções definidas

Feita esta distinção, podemos referir que o investimento na primeira alternativa poderá encontrar maior receptividade em casos de auditoria interna (de empresas com potencial e capacidade para tal) ou, na nossa opinião, em certos tipos de entidades (entidades reguladoras, empresas públicas, por exemplo). No caso da auditoria financeira tradicional temos dúvidas sobre a viabilidade de implantação de uma solução tão abrangente de auditoria contínua nos termos da primeira alternativa apresentada, mas esta questão será abordada mais à frente.

Há várias fases de uma auditoria contínua e os diversos softwares devem ser susceptíveis de dialogar entre eles nas várias fases – obtenção de dados, tratamento de dados, testes de auditoria e relatório de auditoria.

Esquematicamente:

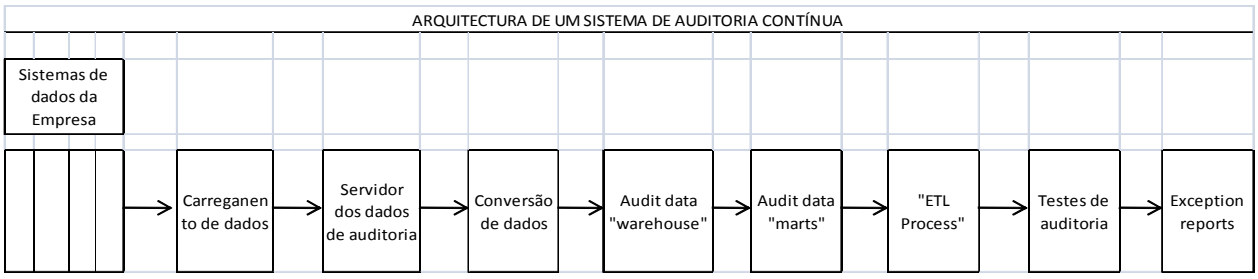

Figura 2 – adaptação do autor, com base em Rezaee et al. (2002)

Desenvolvendo alguns pontos:

- *"Data warehouse"*: é um grande repositório de dados da empresa a auditar com ferramentas para extrair e analisar dados;
- *"Data marts"*: é um repositório mais pequeno relativo apenas a uma área funcional (finanças, compras, vendas, etc.);
- *"ETL process"*: processo de extracção, transformação e carregamento de dados;
- O desenvolvimento de uma arquitectura deste tipo requer uma colaboração profícua entre a direcção de sistemas de informação da empresa e os auditores;
- Podem estar envolvidos custos significativos no desenvolvimento inicial desta arquitectura, com o retorno a ser retirado ao longo do tempo, como qualquer outro investimento;
- Os dados a analisar pelo auditor podem estar em diferentes formatos, não susceptíveis de leitura imediata pelo auditor.

Já referimos atrás que é aconselhada a redução da dimensão dos testes substantivos reforçando o auditor os testes dos controlos. A AICPA no seu SAS nº 80 – *Amendment to SAS nº 31 and Evidencial Matter* – afirma claramente esta opinião favorável ao reforço dos testes aos controlos.

Murcia et al. (2008) apresenta a seguinte comparação de 3 modelos de auditoria contínua[10]:

[10] Citando Flowerday e tal. (2006)

COMPARAÇÃO DE 3 MODELOS DE AUDITORIA CONTÍNUA			
	Modelos		
	Rezace et al.	Onions	Woodroof & Searcy
Exactidão das transacções	Testes de auditoria padrão	Transacções são verificadas à	Dados analisados por meios
	são construídos em "data	data a entrada ou + tarde	integrados no sistema
	marts" (correndo continua	CAATTS: tempo real	Aplicar princípios SYSTRUT
	mente ou em datas	Expert systems:continuamente	
Confiança do sistema	predeterminadas)	Controlo de passwords,logs de	O auditor define as regras
de controlo interno	Uso de CAATS	auditoria, segurança de sistemas	para os agentes digitais
	ITF (integrated test facilities)		
	incluidos		
Tempo real	Objectivo do modelo	Corre em paralelo com sistema	Objectivo do modelo
Método de relato	Dados entregues na workstation	Alertas através de VPN	3 níveis de alertas enviados ao
	do auditor, onde pode gerar	(virtual private networks)	auditor por e-mail
	os seus relatórios		
Formato proposto	Data mart; data warehouse;	Data marts; XCAL	----
	XBRL		

Figura 3 - adaptado de Murcia (2008)

Chan e Vasarhelyi (2011) desenvolvem a temática da metodologia da auditoria contínua começando por diferenciá-la da auditoria tradicional:

		Auditoria tradicional	Auditoria contínua
Frequência		Periódica	Contínua ou mais frequente
Abordagem		Reactiva	Proactiva
Procedimentos		Manuais	Automáticos
Papel/trabalho do auditor		Papeis independentes dos auditores (int. e ext.)	Auditor externo certifica o sistema de aud. contínua
		Grande parte trabalho manual e demorado	Trabalho baseado em "excepções" e julgamento humano
Natureza, extensão e calendário dos testes	N	> Proc. analíticos e testes substantivos	> Testes aos controlos e de garantia continuamente
	E	> amostragem	> toda a população (100%)
	C	> testes aos controlos e testes substantivos têm	> testes aos controlos e testes substantivos têm
		lugar em separado	lugar em simultâneo
Testes		Testes com intervenção humana	Modelos e "data analytics"
Fases		> Planeamento	> Automatização dos procedimentos
		> Trabalho de campo	> Modelização dos dados e
		> Relatório	> Relatório
Reportes		Periódicos	Contínuos ou mais frequentes

Figura 4– adaptado de Chan e Vasarhelyi (2011)

Passemos a analisar cada um dos pontos deste quadro, clarificando a metodologia própria da auditoria contínua:

- Auditoria contínua ou periódica

A auditoria contínua visa assumir o carácter de permanência e em tempo-real em contraponto à auditoria tradicional, que é pontual ou episódica. Porém, este carácter de continuidade não deve ser indiscriminado mas restrito às áreas consideradas de maior risco, por razões de eficiência.

- Auditoria reactiva vs. proactiva

A auditoria financeira tradicional é anual, podendo detectar erros materiais ou fraudes meses depois dos mesmos terem tido lugar; já a auditoria contínua é realizada de um modo mais frequente ou mesmo contínuo, através da detecção de "excepções" e promovendo uma actuação rápida, uma vez as mesmas detectadas.

- Procedimentos manuais vs. automáticos

Na auditoria tradicional predominam os testes manuais; na auditoria contínua os procedimentos são automatizados através do recurso a computador (TAAC). Esta automatização encerra vantagens – redução de custos e maior eficácia e eficiência da auditoria – e eventuais dificuldades – a automatização pode não ser integral, por necessidade intervenção humana (do auditor), standardização dos dados para minimizar a intervenção pessoal e formalização do sistema de controlo interno. Tudo isto no sentido de maximizar a automatização e reduzir a intervenção humana. Na auditoria contínua, as tarefas automáticas são remetidas para o computador, ficando a cargo do auditor as vertentes de julgamento de "cepticismo profissional" (imparidades, depreciações, provisões, por exemplo)[11], além da análise das "excepções" detectadas pelo sistema.

- O papel do auditor (interno e externo)

A efectiva aplicação da auditoria contínua pode vir a acarretar significativas alterações no papel dos auditores (internos e externos) nos anos futuros:

  - ✓ É natural, e assim tem sucedido nos países mais avançados nesta matéria, que a auditoria contínua se inicie pela auditoria interna da empresa; mas,

[11] Com recursos à "inteligência artificial" mesmo alguns destes assuntos de julgamento poderão ser automatizados.

numa fase seguinte, é admissível que venha também a ser adoptada pela auditoria externa ou financeira [12];

- ✓ Assim sendo, poderemos vir a assistir a uma sobreposição das funções dos auditores externos e internos, por recurso ao mesmo modelo de auditoria contínua. A prazo, nesta ordem de ideias, pode vir a ser pedido ao auditor externo que proceda à avaliação e à certificação da efectiva operação do sistema de auditoria contínua da empresa (previamente adoptado para fins de auditoria interna), o que constituirá uma enorme mudança em relação ao seu papel actual. Para tal, o auditor externo terá de avaliar a independência, a objectividade, a proficiência do auditor interno e do modelo de auditoria contínua adoptado;

- ✓ Caso se venha a generalizar o funcionamento da auditoria contínua, o auditor abandonará os testes manuais que tradicionalmente realiza, virando a sua atenção essencialmente para a análise das excepções[13] geradas pelo sistema de auditoria contínua, a avaliação das estimativas contabilísticas e julgamentos;

- ✓ Aos auditores externos no futuro poderá também ser pedido uma espécie de "selo" ou garantia sobre o sistema de auditoria contínua adoptado (atestando também que não foram feitas alterações indevidas ao sistema, etc.), certificando a concepção, a manutenção e o funcionamento do sistema de auditoria contínua da empresa. E poderá realizar comparações de tais sistema com o do *"peers group"* com vista à sua eventual melhoria.

Como se pode comprovar, estamos a considerar funções do auditor bem diferentes das actuais e que poderão levar a alterações profundas na regulamentação e no estatuto dos auditores externos em relação à actualidade.

[12] Numa primeira fase, julgamos ser mais pacífico nas entidades reguladoras e nas empresas públicas.
[13] *"exception reports"*, anomalias ou *outliers.*

- Natureza, extensão e calendário dos testes

Estes aspectos da auditoria sofrem alterações profundas com a introdução da auditoria contínua, como já referimos:

- ✓ Os testes substantivos perdem relevância em relação à monitorização contínua dos controlos internos (procurando detectar violações dos mesmos) e à monitorização dos dados transaccionais (em busca de "excepções");
- ✓ Na auditoria tradicional os testes aos controlos antecedem os testes substantivos; na auditoria contínua, os testes aos controlos e os testes às transacções têm lugar em simultâneo;
- ✓ Na auditoria contínua pode testar-se a totalidade da população, abandonando-se a tradicional amostragem de auditoria.

- *"Data modelling" e "Data analytics"*

Na auditoria tradicional recorre-se a rácios, indicadores, tendências e análise de regressões. Na auditoria contínua são aplicadas aos dados das transacções e às contas da posição financeira técnicas estatísticas, *"machine learning*" e *"data mining",* tais como regressão, classificação, associação e *"clustering".* Quanto à monitorização dos controlos internos, não se usam as "data analytics", mas sim a dicotomia *"compliance/non-compliance".*

- Fases da auditoria contínua

As fases da auditoria contínua resumem-se no esquema seguinte:

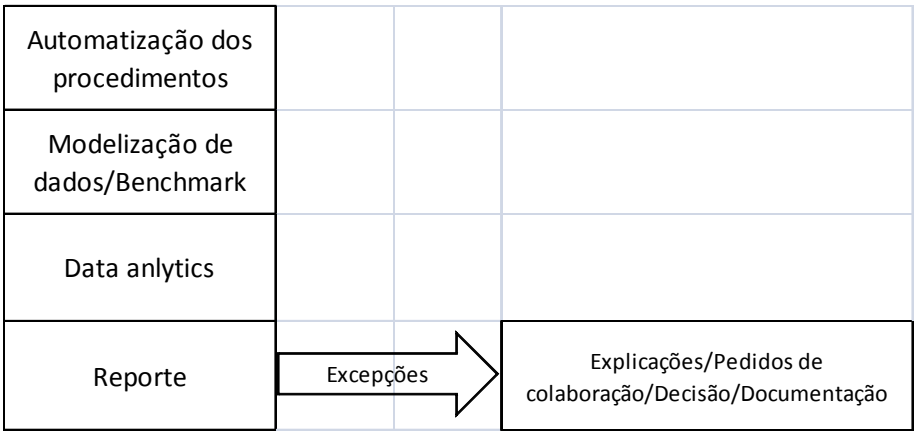

Figura 5 – adaptado de Chan e Vasarhelyi (2011)

Noutros termos, o faseamento da auditoria contínua é o seguinte:

- Identificar as áreas críticas a sujeitar a auditoria contínua;
- Definir o modelo de dados:
  - *"training set"*
  - *"validation set"*
- *"Data analytics";*
- Detecção das "excepções" ou "anomalias

- Relatório de auditoria

Se uma "excepção" é detectada – quer no sistema de controlo interno ou numa transacção – deve ser sanada pela gestão antes da emissão das demonstrações financeiras.

Para que a auditoria contínua funcione com sucesso é necessário respeitar algumas condições representadas na figura seguinte:

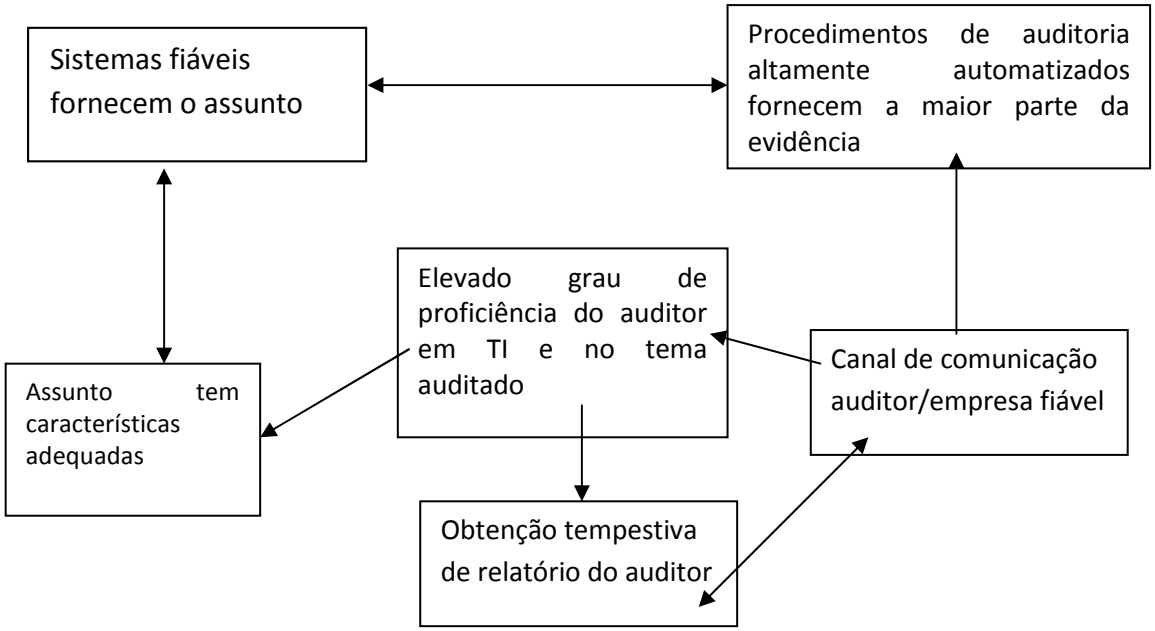

Figura 6 - Fonte: *Continuous auditing*, CICA, 1999

A chamada "evidência" – que é sempre uma pedra de toque para o auditor – sofre alterações significativas com a auditoria contínua. Em particular, com esta última estamos perante uma auditoria sem papéis, surgindo uma "evidência electrónica". Mas, então, o auditor tem de assumir cuidados particulares, porque a evidência que existe num dado momento pode não estar disponível posteriormente – seja porque o programa não permite reconstituir a situação a uma certa data, os ficheiros mudaram ou não há cópias dos ficheiros àquela data.

Por fim, abordemos os testes substantivos e as particularidades que assumem com a auditoria contínua. Como na auditoria tradicional, há três tipos de testes substantivos – os testes às transacções, os testes aos saldos e os procedimentos substantivos.

Os procedimentos analíticos consistem no cálculo de comparações e relações entre dados financeiros e não financeiros - rácios, indicadores, desvios em relação a orçamentos, evoluções históricas. As TI são particularmente adequadas para o cálculo automático fiável destes indicadores, que podem ser potenciados e automatizados ao abrigo da auditoria contínua nas diversas fases – planeamento, recolha de evidência e revisão final.

Os testes às transacções destinam-se a avaliar a regularidade do processamento das transacções e se houve impacto material nas demonstrações financeiras. Sob auditoria contínua, os testes das transacções são realizados continuamente reduzindo-se a sua extensão no final do ano e em paralelo com os testes aos controlos.

Os testes dos saldos, em auditoria contínua – confirmações, inventários, reconciliações, etc - são levados a cabo depois das demonstrações financeiras elaboradas para o auditor expressar uma opinião sobre os mesmos. Aqui também o software de auditoria pode dar uma ajuda preciosa na preparação e elaboração destes testes.

A auditoria contínua cria valor ao libertar o auditor das tarefas mais mecânicas e automáticas (assumidas pelo computador), permitindo que se concentre essencialmente nos temas que requerem julgamento humano.

CAPÍTULO 5 - CONTROLO INTERNO

As investigações realizadas sobre a metodologia da auditoria contínua colocam ênfase na importância acrescida dos controlos internos para a auditoria contínua em relação à auditoria tradicional.

O controlo interno tem sido alvo de tratamento através de vários modelos, enquadramentos (*"frameworks"*) ou estruturas de referência, permitindo-nos destacar os seguintes:

- O *"Internal Control – Integrated Framework"* do COSO, emitido em 1992 e que veio a ser complementado em 2004, através do tratamento específico dado à gestão do risco pelo *"Entreprise risk management (ERM) Framework";* é certamente o modelo mais divulgado e de aceitação mais generalizada a nível internacional;
- O *COBIT – "Control Objectives for Information and related Technologies",* protagonizado pelo ISACA e pelo ITGI*,* com uma terceira edição em 2000, que propõe um modelo de governação para a área dos sistemas de informação;
- O *SAC – "Systems auditabiliy and control",* emitido em 1991 pelo Internal Auditors Research Foundation do IIA (Institute of Internal Auditors), destinado a suportar a actividade dos auditores internos;
- As normas internacionais de auditoria SAS 75 e 78, emitidas em 1988 e 1995, pelo AICPA para servirem de guia à actividade dos auditores externos;
- O *CoCo – "Criteria of control board – Guidance on assessing control – The CoCo principles"*, editado em 1997 pelo The Canadian Institute of Chartered Accountants;
- *ISO 17779 – "Code of practice for information management"*, de 2000, da autoria da International Organization for Standardization.

O conceito de controlo interno [14] é um dos mais importantes para os auditores, sejam internos ou externos.

O IIA define "controlos" como:

- "qualquer acção tomada pela gestão ou qualquer outra parte para gerir risco e aumentar a probabilidade de que os objectivos estabelecidos e as metas serão alcançadas. A gestão planeia, organiza e dirige o desempenho de acções suficientes para fornecer garantia suficiente que os objectivos e metas serão alcançados"

A AICPA no seu SAS nº 1 original apresentava a seguinte definição de controlo interno:

- "controlo interno compreende o plano da empresa e todos os métodos e medidas adoptados para salvaguarda dos activos, verificar a exactidão e fiabilidade dos seus dados contabilísticos, promover a eficácia operacional e encorajar a adesão às políticas de gestão definidas".

O COSO define controlo interno como segue:

- "controlo interno é um processo da responsabilidade do conselho de administração, da gestão executiva ou de outro pessoal da entidade, desenhado para fornecer garantia razoável a respeito da consecução dos seguintes objectivos da organização:
  - Eficácia e eficiência das operações
  - Fiabilidade do relato financeiro
  - Cumprimento das leis e regulamentos aplicáveis"

Com base neste conceito, o COSO utiliza um modelo tridimensional para descrever o sistema de controlo interno de uma entidade.

A crescente evolução e complexidade dos sistemas de informação e das TIC (os potentes ERP designadamente), repetidas vezes referida ao longo deste trabalho, salienta a

[14] Alguns autores defendem que os auditores externos utilizam a expressão "controlo(s) interno(s)" enquanto os auditores internos utilizam apenas o termo "controlos", com o mesmo significado e conteúdo.

questão da abordagem mais adequada do auditor para dar resposta à correcta avaliação do sistema de controlo interno e gestão dos riscos, face à proliferação de dados sob a forma electrónica, reporte financeiro on-line, comércio electrónico e EDI.

Passa a apresentar-se de modo sintético a *"Integrated framework"* do COSO relativa ao controlo interno, esquematicamente representada pelo conhecido cubo:

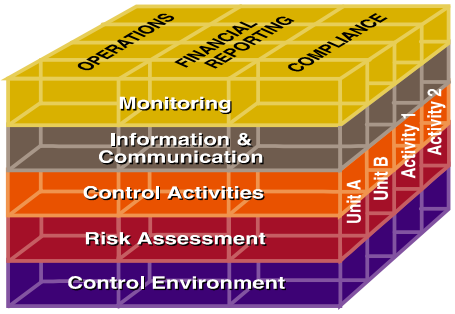

Figura 7 – Fonte: COSO, "Internal Controls – Integrated Framework"

Na face principal estão expostas as 5 componentes principais de um sistema de controlo interno:

1. Ambiente de controlo

O ambiente é fundamental, é a *fundação* de qualquer sistema de controlo interno, porque condiciona todas as actividades, o modo como o risco é avaliado e as restantes componentes e todas as três dimensões e os seus elementos.

O ambiente reflecte a atitude geral e as acções do conselho de administração, da gestão e de todo o restante pessoal sobre o controlo interno.

A história e a cultura da empresa são muito importantes para este ambiente e para sua consolidação.

Nas empresas mais pequenas os factores do ambiente de controlo podem ser mais informais, mas não deixam de ser importantes.

Alguns elementos do ambiente de controlo:

- *Integridade e valores éticos*

A empresa pode apresentar um código de conduta (por exemplo: o juramento de Davos), devendo ser difundidos sinais desta mensagem pela empresa.

A política de incentivos ou de objectivos pode corroer estes princípios e entrar em contradição com eles. Por exemplo: a definição metas irrealistas para vendas pode levar os comerciais a violarem regras apenas para alcançarem as metas.

- *Compromisso com a competência*

Pessoal incompetente pode fazer perigar o ambiente de controlo da empresa. Um departamento de recursos humanos forte, com um sistema de gestão do desempenho adequado e bem gerido é importante.

- *Conselho de Administração (executivo) e Comité de Auditoria*

As suas acções e exemplos têm grande importância para todo o universo da organização.

- *Filosofia de gestão e estilo de operação*

Estes factores dos principais gestores (a diversos níveis) afectam o ambiente. Por exemplo: a "apetência" pelo risco que transmitem.

- *Estrutura organizativa*

A organização: tem a ver com a definição de funções e de relações; o organograma é o documento definidor e representativo da organiação.

- *Atribuição de autoridade e responsabilidade*

Relacionado com o elemento anterior: deve ser atribuída aos colaboradores a respectiva autoridade com a consequente *"accountability"***.** Se as pessoas não sentem esta responsabilização, tenderão a ser mais negligentes.

- *Políticas e práticas de recursos humanos*

Há diversas áreas desta função que devem contribuir poderosamente para o ambiente: contratação, acolhimento, avaliação de desempenho, formação, acção disciplinar, etc. Esta área é crítica para se criar um ambiente de controlo adequado.

2. Avaliação do risco

Os objectivos de uma organização podem estar em risco por diversos factores (internos e externos). Uma empresa deve ter um processo para avaliar os riscos potenciais que possam por em causa a consecução dos seus objectivos.

Esta avaliação de risco distingue-se da *framework* ERM (a estudar à frente) :

- Foca-se nos controlos internos da empresa;
- Tem um âmbito muito mais estreito que o COSO ERM.

Esta avaliação é um processo de 3 passos:

- Estimar a significância (impacto) do risco;
- Avaliar a probabilidade de ocorrência;
- Definir como o risco deve ser gerido e que acções tomar.

Esta *framework* do COSO considera que os riscos devem ser considerados em 3 perspectivas:

i. Riscos devidos a factores externos (a desenvolver no capítulo seguinte):
   - ✓ Alterações tecnológicas;
   - ✓ Mudança nos hábitos e gostos dos clientes;
   - ✓ Nova legislação ou regulamentos;
   - ✓ Acidentes naturais ou catástrofes.

ii. Riscos devidos a factores internos:
   - ✓ Rotura num servidor;

- ✓ Competência dos recursos humanos contratados;
- ✓ Facilidade de acesso do pessoal aos activos;
- ✓ Riscos de actividades específicas;
- ✓ Os riscos também ser encarados por actividades (finanças, marketing, TI, etc.) ou unidades de negócios.

3. Actividades de controlo

Actividades de controlo são os procedimentos e políticas a todos os níveis de uma organização, podendo ser de diversos tipos:

- ✓ Revisões de nível superior: comparações com orçamentos, estatísticas, dados da concorrência, medidas de benchmark, etc. (Sistema de gestão orçamental);
- ✓ *"Exception reports"* relativos a diversas actividades, como:
  - TI: tentativas de acesso não autorizados
  - Auditoria contínua
- ✓ Controlos físicos
- ✓ Segregação de funções
- ✓ Supervisão e conferências independentes
- ✓ Indicadores de desempenhos
- ✓ Os controlos sobre TIC são críticos. Por exemplo: *"exception report*" se nº horas de um trabalhador por semana > 80h.

Estas actividades de controlo devem estar relacionadas com os riscos identificados (2.)

4. Comunicação e informação

Embora relacionados, comunicação e informação são componentes diferentes do ambiente de controlo interno. Deve haver informação adequada (assente em TI) a circular para cima e para baixo de uma empresa. As empresas devem também ter procedimentos de comunicação para comunicar com as partes internas e externas.

✓ Informação

Uma empresa dá informação a todos os níveis para alcançar os seus objectivos e esta informação deve fluir ao longo da empresa. Exemplo: para preparar as demonstrações financeiras.

O COSO considera "sistema de informação" seja ele manual, automatizado ou conceptual, formal ou informal. Exemplos.: conversa com clientes ou fornecedores são fontes de informação informais (uma empresa eficiente deve ter sistemas de informação apurados para obter informações dos seus clientes: pedidos, sugestões, reclamações, etc.).

Os sistemas de informação apurados são vitais para uma empresa se adaptar ao clima de

mudança e incerteza de hoje. Serão a TI de uma empresa adequadas às suas necessidades de hoje? As TI começaram nas empresas na contabilidade e finanças nos anos 50 (máquinas IBM) e só depois se expandiram para outras áreas empresariais.

O COSO aconselha que nos dias de hoje se implementem SI estratégicos e integrados – *estratégicos* (como parte da estratégia da empresa e no respeito da mesma) e *integrados* (sistema de controle produção, de máquinas, de inventários, da expedição, etc).

A qualidade da informação é também essencial – o seu conteúdo, a sua tempestividade, a sua correcção ou exactidão e a sua acessibilidade ou disponibilidade.

✓ Comunicação

A empresa deve definir os canais de comunicação adequados para comunicar quer internamente quer com o exterior.

A comunicação é entendida nos dois sentidos:

- Componente interna

Todos os *stakeholders* devem receber mensagens da gestão lembrando-lhes da sua responsabilidade no controlo interno da entidade, os canais podem ser normais ou confidenciais (*"whistleblower programs"* ou de comunicação de irregularidades).

- Componente externa

Comunicação com clientes (fonte preciosa), accionistas, bancos, Bolsa, fornecedores, reguladores, etc; o relato financeiro como canal fundamental; a Web como canal privilegiado hoje em dia.

- Meios

Diversos meios podem ser usados: boletins, sites, webcast, vídeos, etc.

5. Monitorização

A monitorização do sistema de controlo interno foi a tarefa tradicional dos auditores internos. Com a *framework* do COSO, esta componente tem um alcance mais amplo: numa óptica dinâmica, já que um bom controlo interno numa altura pode não o ser noutra.

A monitorização destina-se a avaliar a eficácia de todas as componentes do sistema de controlo interno e a implementar acções correctivas quando reveladas necessárias.

A distinguir:

- Actividades de monitorização permanentes (*"ongoing"*)

O COSO salienta a importância destas actividades, isto é, funções de rotina que executam esta monitorização. Exemplos:

- ✓ Comunicações de terceiros; por exemplo: nº de telefone para reclamações de clientes;
- ✓ Actividades de supervisão (mesmo a níveis intermédios);
- ✓ Inventários (de stocks, de activos fixos, reconciliação de activos);
- ✓ Funções normais de gestão: reportes regulares, *"exception reports"*, etc

- Avaliação separada do sistema de controlo interno

São frequentes quando se fazem aquisições, mudança no negócio, por exemplo.

- Reporte de deficiências do sistema de controlo interno

Seja qual for o meio de detectar os pontos fracos do sistema de controlo, estes devem ser reportados à gestão.

Coloca-se a questão do detalhe do reporte e do destinatário do mesmo. O COSO diz: "àqueles que podem tomar a acção necessária" e precisa: "devem ser reportados não só ao responsável pela função mas também pelo menos um nível acima".

Outra questão importante é a relação entre materialidade e auditoria interna. O COSO defende que não deve vigorar em auditoria interna o critério da materialidade, diferentemente do que sucede na auditoria externa ou financeira. "Um erro é um erro", um mau exemplo propaga-se para o restante pessoal, mesmo que não seja material.

A *framework* de controlo interno do Coso é tridimensional, não se podendo esquecer as outras duas dimensões, para lá das componentes que abordámos até aqui. Assim, todas as componentes abordadas até aqui devem ser consideradas em relação com as outras duas dimensões:

- dimensão superior do "cubo": fiabilidade do reporte financeiro, conformidade com leis e regulamentos e eficácia e eficiência das leis e regulamentos
- unidades ou actividades desempenhadas pela organização

Este *framework* do COSO tem vindo a tornar-se um padrão mundial em termos de controlo interno.

Ao falar-se em modelos de referência de controlo interno, não podemos deixar de abordar também sucintamente o chamado COBIT – Control Objectives for Information and related Technologies.

O COBIT – criado em 1996 pelo ISACA [15] e pelo ITGI [16] - encerra o conjunto das melhores práticas para a gestão de TI, visa definir um modelo de governação de TI. Elementos-chave da governação de TI são valor, risco e controlo.

Pretende dar resposta a várias questões, nomeadamente: como medir o valor criado pelas TI numa organização? Como gerir os riscos relacionado com as TI ?

O COBIT concentra-se em 5 *áreas* de foco – alinhamento estratégico, criação de valor, gestão do risco, gestão de recursos, medida do desempenho - representadas no polígono seguinte:

Figura 8 – Fonte: COBIT

[15] Information Systems Audit and Control Association
[16] IT Governance Institute

e em quatro *domínios*:

- planear e organizar - destacam-se a estratégia de IT, arquitectura de IT, gestão do investimento e recursos humanos de IT;

- adquirir e implementar – destacam-se a identificação de soluções, a aquisição e manutenção do software e a operação do sistema;

- entregar e apoiar – destacam-se os níveis de serviço, a gestão do desempenho, a formação dos utilizadores e gestão da operação do sistema;

- monitorizar e avaliar – salienta-se a governação de IT.

Segundo o COSO, "gestão do risco[17] é um processo efectuado pela administração executiva de uma entidade, gestão e outro pessoal, aplicado na definição estratégica e através da empresa, com vista a identificar potenciais eventos que podem afectar a entidade e gerir o risco para que este esteja dentro do seu apetite (apetência) ao risco, para fornecer razoável segurança a respeito da consecução dos objectivos da entidade".

Esta nova Framework desenvolvida pelo COSO foi apresentada em 2004, na sequência de escândalos financeiros gritantes de início da década de 2000 (Enron e Worldcom, sobretudo).

Esta estrutura de referência não veio anular a emitida em 1997, designada por *"Internal Control – Integrated Framework"* e analisada no capítulo anterior, veio integrá-la no seu seio, conferindo um âmbito mais lato ao conceito tradicional de controlo interno.

Aparentemente muito similar à anterior Framework, mesmo esquematicamente, esta ERM Framework não teve ainda o tempo suficiente de maturação e de aplicação, tal como a *Internal Control - Integrated Framework* já teve.

Figura 9 – Fonte: COSO, ERM, Entreprise Risk Management – Integrated Framework

[17] ERM em inglês: entreprise risk management

Num ambiente de tão acentuadas mudança e incerteza, as empresas precisam de identificar os riscos que enfrentam, sejam de que ordem forem – financeiros (subida de taxas, falta de crédito), operacionais, sociais, ambientais, políticos, tecnológicos, naturais, de mercado (alteração de gostos) - para os gerir a um nível aceitável.

A gestão de risco é um meio de as empresas obterem protecção contra a incerteza. A gestão de riscos de uma organização conseguirá atingir o seu objectivo, alinhando o "apetência para o risco" com a sua estratégia/objectivos, seleccionando as melhores respostas a dar aos riscos, reduzindo as surpresas e prejuízos operacionais, aproveitando oportunidades e optimizando a afectação do capital.

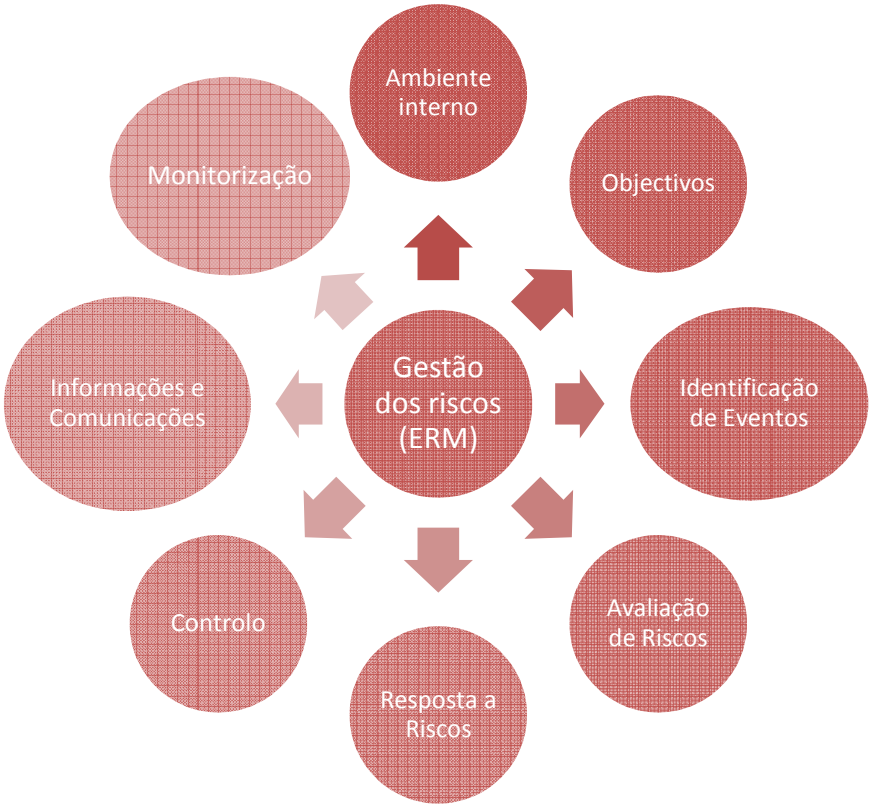

Figura 10 – Esquema de componentes da ERM do COSO, adapt. do autor

Passamos a abordar sinteticamente estas componentes do modelo de ERM do COSO.

1 . Ambiente interno

O ambiente interno é a base dos outros componentes da gestão de riscos. Enquanto a *framework* do Controlo Interno se foca em práticas correntes, esta ERM aponta sobretudo para o futuro. Compreende factores como: a cultura da empresa, valores éticos e integridade, não apenas palavras, mas sobretudo as acções apercebidas (os exemplos), traduzindo uma atitude quanto a riscos.

Este ambiente é que determina o modo como os riscos são identificados, avaliados e geridos em cada empresa, aos mais diversos níveis. Tudo isto é que determina a apetência para o risco de cada empresa – a quantidade de riscos que está disposta a aceitar para criar valor.

Os administradores não-executivos, como maioria do conselho de administração, desempenham um papel relevante no controlo dos eventos de risco, de accordo com as mais recentes regras e princípios de *corporate governance*.

A competência dos recursos humanos é um factor determinante para contribuir para uma ambiente favorável em termos de gestão do risco, tal como as políticas de recursos humanos em diversas áreas – na contratação, no acolhimento, na formação, na avaliação de desempenho.

A estrutura organizacional é também importante para este ambiente interno, através da clareza que define para cada colaborador na sua autoridade e na responsabilização (*"accountability"*).

2 . Definição de objectivos

Os objectivos são prévios à gestão dos riscos, constando das declarações de missão, de visão e dos objectivos estratégicos definidos. Compete à gestão assegurar que os objectivos estão alinhados com a apetência a risco.

Uma correcta gestão dos riscos corporativos não define os objectivos, antes devendo assegurar que esses objectivos estejam dentro dos limites de apetência para o risco definidos (que os riscos não sejam excessivos nem demasiado baixos).

3. Identificação de eventos

São identificados os eventos que poderão afectar a organização em termos positivos (*oportunidades*) ou negativos (*ameaças*), podendo ser de origem interna ou externa.

Há diversas técnicas de identificação dos eventos - inventário (arquivo) de eventos; análise interna (reuniões com responsáveis de negócios); entrevistas, inquéritos, estudos (por exemplo: sugestões de clientes, colaboradores, etc); alçadas e limites (sinais de alerta; exemplo: preços da concorrência), seminários e entrevistas com facilitadores (exº: seminário liderado por perito); análise de fluxo de processo, indicadores preventivos de eventos (exemplo: financeiras actuam a tempo para evitar incumprimento); metodologias de dados sobre eventos de perda; "despoletadores" (exemplo: mais do que 5 tentativas de intrusão no sistema por semana desencadeia investigação).

4. Avaliação de riscos

Identificados os riscos, trata-se agora de avaliar em relação aos mesmos a sua probabilidade (quantitativa ou qualitativa - alta/média/baixa) e o seu impacto (exemplo: custo de falha do servidor pode estimar-se: custo da substituição, de restaurar o sistema, das vendas perdidas, etc).

O risco inerente é o risco a sofrer na ausência de medidas de gestão do risco; o risco residual: é o risco que resta após as medidas da gestão para contrariar esse risco.

A filosofia do ERM não pretende fazer uma quantificação muito exacta dos riscos. A ideia é efectuar um ranking dos riscos atendendo aos 2 factores (probabilidade e impacto), numa escala (1 a 10, por exemplo).

5. Resposta a riscos

Como vai responder a gestão aos riscos detectados e avaliados? Quatro atitudes podem ser adoptadas: evitá-los, reduzi-los, compartilhá-los ou aceitá-los.

A resposta que se irá adoptar deverá permitir à empresa manter o *risco residual* dentro da tolerância a risco desejada.

6. Actividades de controlo

Estas actividades são as políticas e procedimentos que visam assegurar que as respostas aos riscos sejam executadas a todos os níveis da organização e em todas as áreas. Exemplos – autorizações; verificações, aprovações e supervisões; reconciliações; segurança e controlos físicos; segregação de funções; *audit trails;* documentação dos processos; indicadores de desempenho

7. Informação e comunicação

Informação e comunicação ligam as restantes sete componentes desta *framewok*. Uma organização carece de informações (de fontes internas e externas) de apoio ao seu sistema de gestão de riscos e a aos mais diversos níveis da organização. Tem muito a ver com tecnologias de informação. Estas informações devem revestir-se de algumas qualidades críticas – conteúdo, exactidão, disponibilidade e tempestividade.

Quanto a comunicações, a ERM deve ser comunicada a todos os *stakeholders*, através dos seguintes canais:

- Internos: a cultura da empresa, os objectivos da organização, a filosofia de gestão dos riscos corporativos, a apetência e a tolerância a riscos; as funções de cada um nestas políticas e procedimentos
- Externos: informação financeira, CRM, índice de satisfação de clientes, via Web.

8. Monitorização

Monitorizar consiste em verificar como todas as componentes da ERM funcionam. A gestão dos riscos empresariais deve ser regularmente monitorizada, avaliando-se o funcionamento dos seus diversos componentes no decurso do tempo. Esta tarefa pode ser realizada pela empresa (de modo regular) ou de modo independente (periodicamente).

Alguns tipos de actividades de monitorização - mecanismos *"ongoing"* (sem esperar pelo fim do mês) tais como reportes sobre disponibilidades, indicadores financeiros, etc; mecanismos periódicos (items em suspenso, tendências, desvios, comparações (com passado ou benchmarks) etc; relatórios de auditoria interna (certamente a melhor fonte).

Analisámos até aqui face frontal do "cubo", mas não podemos esquecer as outras 2 faces.

Cada componente do ERM funciona em três dimensões, incluindo também:

- ✓ Objectivos: operacionais, estratégicos, de *compliance* (com leis, regulamentos, regulações, etc.)
- ✓ Organização: ERM deve cobrir todas as unidades de uma dada organização.

CAPÍTULO 7 - TECNOLOGIAS DE INFORMAÇÃO

Os actuais sistemas de informação estão suportados esmagadoramente pelas novas TIC de graus de complexidade e sofisticação crescentes.

Já salientámos o impacte sobre a auditoria que os novos sistemas de informação comportam - designadamente em termos da produção de dados em forma digital, do e-commerce, da produção que se vai observando de relato financeiro on-line e do EDI. Quer a auditoria interna quer a auditoria externa têm de se adaptar e dar resposta a estes novos condicionalismos.

Uma das questões de maior acuidade que se coloca é da capacidade da auditoria para dar resposta num prazo muito mais curto (para não falar em resposta em "tempo real"). Outro ponto a salientar é o desaparecimento de documentos físicos que possam servir de evidência, substituídos por suportes electrónicos.

Ahmed (2007) no seu estudo que teve por objecto os departamentos de auditoria interna de 250 empresas cotadas no London Stock Exchange[18], conclui pela necessidade de os auditores internos deterem competências para além da contabilidade para satisfazerem as expectativas da gestão de topo e dos comités de auditoria. Dos auditores internos é esperada a criação de valor através da apresentação de recomendações e actuando como consultores. Este autor cita o IIA quando este foca o crescente papel da auditoria interna nas últimas décadas dentro das organizações como um serviço profissional essencial quer para o interior (administração e direcção) quer para o exterior (*stakeholders* e reguladores). Quer os utentes externos quer internos procuram efectiva gestão de risco para mitigar a exposição a riscos potenciais e a eficiência do controlo e da governação. O ambiente actual das empresas e organizações em termos de TI (designadamente em termos de relato financeiro on-line, de comércio electrónico, de EDI, etc.) comporta riscos inerentes tais como acessos não autorizados, acessos remotos e fraudes. Neste ambiente, é esperado da auditoria interna que apoie a gestão em termos de garantia do controlo interno, avaliação contínua da fiabilidade da informação financeira, tanto quanto possível

[18] Este estudo teve, contudo, uma limitação significativa que foi a baixa taxa de resposta (apenas 4%) por razões de confidencialidade.

em “tempo real”. Neste estudo, o autor esquematiza do modo seguinte o impacto dos sistemas de informação na auditoria interna:

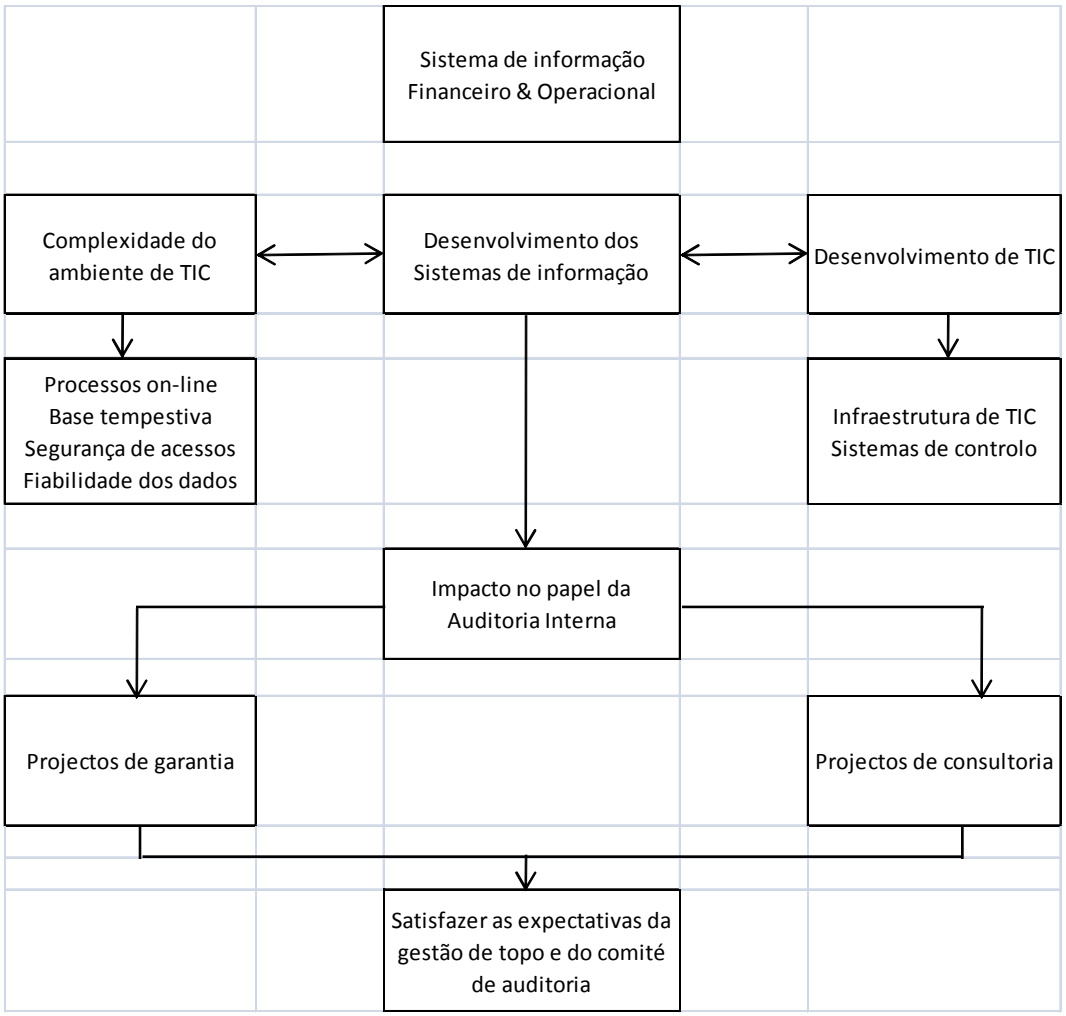

Figura 11 - adaptado de Ahmed (2007)

As TI têm vindo a tornar-se crescentemente complexas e sofisticadas. Nos anos 1990 assistiu-se à implementação dos ERP[19] , cada vez mais utilizados nas empresas. Estes sistemas podem dificultar a chamada *“audit trail”*[20] , o que pode ser ultrapassado pelo auditor com o recurso acrescido a TAAC.

[19] Enterprise Resource Planning
[20] “audit trail” significa, para o auditor, seguir manualmente uma transacção desde o seu documento de origem até à sua entrada ou lançamento nos registos contabilísticos.

O advento dos ERP constituiu um marco - a par de outros factores e eventos – para a consolidação da auditoria contínua. Com efeito, há uma relação entre os dois e um caminho paralelo e interacção entre a automação e desenvolvimento visados pela auditoria contínua e a integração dos processos de negócios e o desenvolvimento dos ERP.

Esta última afirmação, e a conjugação entre TIC e auditoria, remetem-nos directamente para o objectivo da auditoria contínua e para o seu potencial de desenvolvimento futuro como um novo paradigma de auditoria, tema central do presente trabalho.

CAPÍTULO 8 - CONSIDERAÇÕES FINAIS

O tema auditoria contínua reveste-se de vincada actualidade quer para académicos quer para práticos da área da auditoria, como foi possível constatar ao longo deste trabalho.

Tendo começado a ser levantado no início da década de 1990 – há apenas 20 anos, portanto – podemos afirmar que se trata de um assunto de plena actualidade na área de interesse da auditoria. Trata-se em grande medida de adaptar o paradigma da auditoria (ou dos diversos tipos de auditoria) à evolução tecnológica, em particular à área dos sistemas de informação.

Estamos perante um tema com um enorme potencial de investigação. O *"Study Group"* (1999)[21] elencou nada menos do que 33 tópicos de investigação, designadamente – a procura de auditoria contínua; requisitos para realizar testes substantivos em auditoria contínua; aplicação de TAAC em auditoria contínua; natureza, extensão e calendário de testes substantivos em auditoria contínua; formato e conteúdo dos relatórios de auditoria contínua; materialidade e nível de segurança em auditoria contínua.

Assim, faz sentido e é oportuno levantar é a seguinte questão: em que medida poderia a auditoria contínua, se estivesse em aplicação, ter evitado ou contribuído para minorar os efeitos de grandes escândalos financeiros internacionais - Worldcom, Enron, Parmalat, etc - e nacionais - BPN, BCP, BPP - ou a crise financeira de 2008 ?

Claro que a auditoria contínua não detecta algumas transacções que não estão registadas nas demonstrações financeiras (operações em *off-shores*, etc.). Mas a auditoria contínua poderia ter contribuído para minorar os desastrosos efeitos daqueles eventos, quer incorporando alguns dos processos no seu modelo (tal como o controlo do cash-flow e das suas dificuldades, definindo diversas "excepções" ou "anomalias" de diversos tipos e emitindo alertas imediatos para o auditor) e, sobretudo, teria permitido antecipar no tempo a detecção dos problemas e anomalias. Cada vez mais, nos dias que correm, os

[21] "Study Group", 1999, *Research report:continuous auditing,* Canada, CA e AICPA

diversos *stakeholders* - não só os gestores, mas também os accionistas, investidores, fornecedores, bancos, colaboradores - precisam de serviços de garantia fornecidos por uma terceira parte independente e objectiva, não bastando já a informação histórica, por vezes já muito atrasada.

A mudança de paradigma da auditoria em direcção à auditoria contínua não será isenta de obstáculos e de dificuldades - tais como os investimentos necessários (não sendo pacífica a análise do retorno de um investimento deste tipo); a necessidade de apoio da gestão; o domínio de novas competências, a disponibilidade de uma infra-estrutura tecnológica e, em termos latos, a substancial mudança de paradigma que está em causa. Como vantagens da auditoria contínua apontam-se as seguintes: ser mais tempestiva, mais exacta, exigir menos custos de funcionamento e ser mais compreensiva.

Foi referido no presente trabalho que a auditoria contínua tende a implantar-se começando pela auditoria interna das empresas, podendo o seu modelo vir a ser acolhido, numa fase posterior, pelos auditores externos de tais empresas.

O início da adopção da metodologia da auditoria contínua pelo auditor externo colocaria desde logo a questão significativa de quem suportaria tal investimento e há que ter também em atenção, como salienta Warren (2007), que os executivos são relutantes a permitir que os auditores externos instalem um processo de auditoria contínua nos seus sistemas por causa das suas preocupações que estes sistemas possam corromper os dados da empresa e reduzir a eficiência operacional do sistema da empresa; acresce que surge uma questão de independência se os auditores externos são autorizados a embeber software de auditoria contínua no sistema de informação de uma empresa. Nos Estados Unidos, foi mesmo levantada a questão se as regras de independência estabelecidas pelo Sarbanes-Oxley Act proibem o auditor externo de implementar um sistema de auditoria contínua num cliente.

Situada no ponto de encontro da auditoria com as TIC, a auditoria contínua virá a constituir-se certamente, de modo gradual, ao longo dos próximos anos, como o novo paradigma de auditoria.

Este trabalho não teve a pretensão de efectuar um desenvolvimento exaustivo do tema - relativamente recente e objecto de crescente interesse da parte de diversos actores – mas proceder a um ponto de situação credível da temática e suscitar desenvolvimentos e investigações futuras, que porventura o próprio autor levará a cabo. Seria particularmente interessante investigar esta temática através de um inquérito dirigido aos responsáveis de auditoria interna de empresas relevantes na matéria, bem como a outros profissionais e a académicos ligados à auditoria.

REFERÊNCIAS BIBLIOGRÁFICAS

- Ahmed, Hany B. (2007). *Information Systems development and the changing role of internal audit*. Disponível em http://ssrn.com/abstract=1324159.
- Alles, Michael; Kogan, Alexander; Vasarhelyi, Miklos (2004). *Continuous reporting and auditing: opportunities and challenges.* Wall Street Lawyer.
- ASB e CICA (1999). *Continuous auditing*
- Chan, David Y. e Vasarhelyl, Miklos A. (2011). *Innovation and Practice of Continuous Auditing.* International Journal of Accounting Information Systems.
- Chou, Charles Ling-yu; Du, Timon; Lai, Vincent S. (2006). *Continuous auditing with a multi-agent system,* Science Direct, Elsevier.
- Coderre, David (2009). *Internal audit efficiency through automation.* New Jersey: John Wiley & Sons.
- Gupta, Parveen P. (2009). *COSO 1992 Control Framework and management reporting on internal control: survey and analysis of implementation practices.*
- Moeller, Robert (2009). *Brink's Modern Internal Auditing*. 7ª edição. New Jersey: John Wiley & Sons.
- Moeller, Robert (2010). *IT Audit, Control and Security*. New Jersey: John Wiley & Sons.
- Murcia, Fernando Dal-Ri; Souza, Flávia Cruz de; Borba, José Alonso (2008). *Auditoria Contínua: uma revisão da literatura.* Organizações em contexto, Ano 4, nº 7, Junho.

- Rezaaee, Zabihollah; Sharbatoghlie, Ahmad; Elam, Rick e McMickle, Peter L. (2002). *Continuous auditing: building automated auditing capability.* Auditing, Março (147-163).
- Rezaaee, Zabihollah; Sharbatoghlie, Ahmad; Elam, Rick (2001). *Continuous auditing: the audit of the future.* Managerial auditing journal, 16/3, (150-158).
- Santos, Carlos A. L. (2009). *Modelo conceptual para auditoria organizacional contínua com análise em tempo real.* Penafiel: Editorial Novembro.
- Warren, J Donald; Smith, L Murphy (2006). *Continuous Auditing: an effective tool for internal auditors.* Internal auditing - Março/Abril (27-35).
- Zhao, Ning; Yen, David; Chang, Chiu (2004). *Auditing in the e-commerce era*. Information Management & Computer Security, V. 12, Nº 5, (389-400).