Da Framework CEO à Auditoria de Sistemas de Informação

Carlos Santos
ISCA-UA/CEO-INESC, Aveiro, Portugal
carlos.santos@isca.ua.pt

André Vasconcelos
CEO-INESC, Lisboa, Portugal
andre.vasconcelos@ceo.inesc.pt

José Tribolet
CEO-INESC, Lisboa, Portugal
jose.tribolet@ceo.inesc.pt

Resumo

Neste trabalho debruçamo-nos sobre a problemática do controlo interno dos processos de negócio com recurso a mecanismos de controlo externos aos processos. Estes mecanismos têm como objectivo assegurar a auditabilidade dos processos de negócio, garantindo que os seus objectivos são atingidos com razoável certeza.
A atenção crescente que tem vindo a ser dada ao controlo interno é motivada por vários factores internos e externos às organizações devido principalmente aos escândalos financeiros que têm surgido, um pouco por todo o mundo, e à proliferação das novas tecnologias de informação como suporte aos sistemas de informação.
A evolução que se tem vindo a verificar no controlo interno, designadamente a alteração no seu comportamento organizacional, de *estrutura* para *processo*, tem-no tornado mais abrangente e dinâmico. Esta tendência evolutiva, em nossa opinião, permite-nos propor que a engenharia organizacional se comece a preocupar com o estudo do controlo interno numa perspectiva científica, com recurso a modelos consistentes e coerentes.
Neste trabalho fazemos inicialmente uma breve exposição sobre o controlo interno e a sua evolução, propondo de seguida a extensão da "framework" CEO com recurso ao modelo COSO para que possa suportar a modelação de mecanismos de controlo interno.

Palavras-chave: "Framework" CEO; COSO; Processos de negócio; Sistema de controlo interno; Auditoria de sistemas de informação.

1 INTRODUÇÃO

De acordo com a teoria de auditoria, uma organização não só precisa de um sistema de informação, mas também de um sistema de controlo interno para assegurar a credibilidade da informação registada e para controlo de potenciais erros. Face ao exposto podemos concluir que uma organização, em simultâneo com os objectivos estratégicos e operacionais, precisa de cumprir objectivos de controlo suportados por processos de controlo.

Com este trabalho pretende-se contribuir para promoção da auditabilidade dos sistemas de informação numa perspectiva holística do negócio utilizando a "*framework*" CEO [FCEO]. Embora o metamodelo da FCEO proposto por [Sinogas 2002] especifique uma associação "***controls***", é necessário proceder a ligeiras alterações, no sentido da evolução da referida "*framework*", para que a mesma possa passar a suportar a modelação de mecanismos de controlo interno. A utilização da FCEO acontece na sequência do trabalho realizado por diversos investigadores [Castela 2001; Mendes 2001; Vasconcelos 2001; Aveiro 2002; Sinogas 2002] em que é demonstrado que a FCEO é suficientemente consistente e coerente, satisfazendo um requisito fundamental para poder suportar um sistema de controlo interno.

O presente artigo está assim estruturado: na secção seguinte fazemos uma breve exposição sobre o controlo interno e a sua evolução; na secção 3 fazemos uma revisão do estado da arte da modelação do controlo interno; na secção 4 é apresentado o modelo COSO; a relação entre a "framework" CEO e o controlo interno de processos de negócio é mostrada na secção 5;

finalmente, na secção 6 são apresentadas as conclusões a que chegaram os autores e são estabelecidas linhas orientadoras que poderão ser úteis em futuros trabalhos de investigação relacionados com esta problemática.

2 TEORIA DO CONTROLO INTERNO

É comum designar por sistema de controlo interno o conjunto de regras, políticas e procedimentos [mecanismos de controlo], envolvidos na gestão do risco empresarial [Pathak 2003].

Um mecanismo de controlo ajuda a atingir o objectivo de um processo sem ser necessariamente parte do processo, figura 1 [O'Connel 1999]. Estes mecanismos são recursos que têm por objectivo, quando utilizados pelos processos, eliminar ou minimizar os riscos.

Um controlo é designado interno quando é um mecanismo interno de uma entidade. O controlo interno pode ser uma excelente ferramenta para que os objectivos de uma organização sejam atingidos. Contudo, a sua implementação necessita de uma "*framework*" coerente [Curtis and Wu 2000].

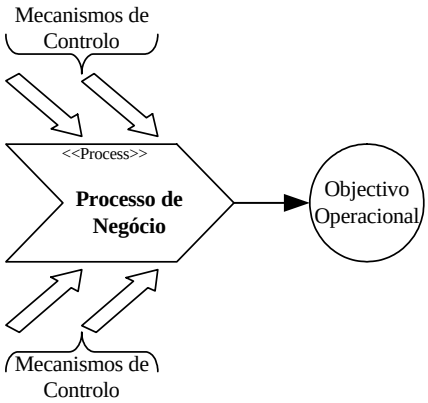

Figura 1 – Os processos de negócio que permitem atingir um objectivo operacional necessitam de ser controlados através de mecanismos de controlo externos ao processo.

Embora o princípio da conservação da energia e da matéria "*...nada se cria, nada se perde, tudo se transforma...*" tenha directo significado nas organizações e consequentemente nos seus sistemas de informação, o mesmo não tem sido completamente entendido, muito menos aplicado, no controlo dos sistemas de informação.

Se tivermos presente este princípio fundamental da física e se fizermos a sua transposição para os sistemas de informação deveremos considerar que a uma "*transacção directa*" corresponderá sempre uma "*transacção indirecta*" para garantir o equilíbrio do sistema de informação figura 2.

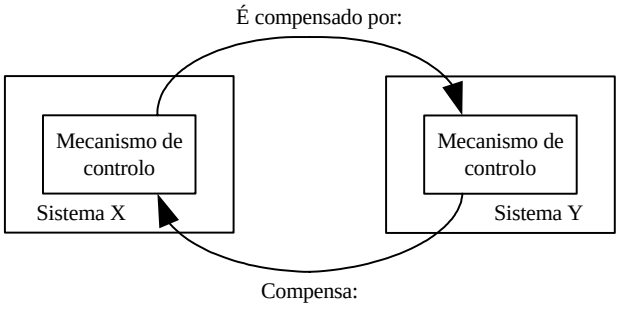

Figura 2 – O processo de controlo para produzir um recurso de controlo recebe informação de duas transacções a "*transacção directa*" e a "*transacção indirecta*".

Como exemplo consideremos o procedimento de delegação de competências frequentemente usado nas organizações e gerador de desequilíbrios. O acto de delegar configura uma "transacção directa" que deve ser compensada por um acto de controlo sobre os agentes que passam a ter a responsabilidade da execução da tarefa. O acto de controlo configura uma "transacção indirecta". Se o acto de delegar não for acompanhado do acto de controlo, não existe compensação e o sistema deixa de estar em equilíbrio.

3 MODELOS DE CONTROLO INTERNO

Existem vários modelos de controlo interno [Champlain 1998], normalmente desenvolvidos por organizações profissionais. A seguir são apresentados seis importantes documentos sobre controlo interno [Colbert and Bowen 2002]:

- ***COBIT*** – "*Control Objectives for Information and Related Technology*", editado por "*Information Systems Audit and Control Foundation*", em terceira edição datada de 2000. É uma "framework" que proporciona uma ferramenta para que os titulares dos processos de negócio possam cumprir eficiente e efectivamente as suas responsabilidades de controlo sobre os sistemas de informação;
- ***SAC*** – "*Systems Auditability and Control*", editado em 1991 por "*Internal Auditors research Foundation*" e revisto em 1994. Dá suporte aos auditores internos no controlo e na auditoria de sistemas de informação e tecnologia;
- ***COSO*** – "*Internal Control – Integrated Framework*", editado em 1992 pelo "*Committee of Sponsoring Organizations of the Treadway Commission*". Faz recomendações para a gestão de como avaliar, relatar e melhorar os sistemas de controlo;
- ***SAS 55 e 78*** – "*Statements on Auditing Standards*", editados respectivamente em 1988 e 1995 por "*American Institute of Certified Public Accountants*". Proporcionam um guia para os auditores externos relativamente ao impacto do controlo interno no planeamento e execução de auditoria das demonstrações financeiras;
- ***CoCo*** – "Criteria *of Control Board – Guidance on Assessing Control – The CoCo Principles*", editado em Junho de 1997 por "*The Canadian Institute of Chartered Accountants*".

Para além dos seis documentos anteriormente indicados, é oportuno fazer-se referência a um outro documento:

- ***ISO 17799*** – "*Code of Practice for Information Management*", editado em 2000 por "*International Organization for Standardization*".

Qualquer um dos modelos referidos pode ser utilizado no desenho e implementação de um sistema de controlo interno, não havendo obrigatoriedade de aplicação de qualquer um deles em particular. No entanto, o modelo COSO para além de ser o único dos modelos referenciados que tem como foco toda a organização, tem várias referências à sua universalidade e também o facto de ter sido introduzido pela Comissão Europeia como modelo de suporte ao seu sistema de controlo interno [Moran 2001]. É ainda aceite por grande parte dos profissionais de auditoria que uma estrutura de controlo efectiva sob o modelo COSO aumentará as possibilidades de um sistema de informação fiável, para ser usado pela gestão e pelo conselho de directores, em particular se for adoptada a sua definição de controlo [Hermanson 2003].

4 O MODELO COSO

O modelo COSO – "*Internal Control – Integrated Framework*" editado por "*Committee of Sponsoring Organizations of the Treadway Commission*" estabelece uma sequência de eventos para a gestão de processos de negócio em ambiente de controlo [Namee 1997]:

- Definição dos objectivos da organização;
- Avaliação do risco;
- Determinação dos controlos necessários.

Um modelo de controlo interno quando aplicado com cuidado, discernimento e visão pode ser a base de um sistema de controlo interno que suporte directamente o sucesso da organização. Se aplicado mecanicamente, o sistema de controlo interno resultante pode suportar um bom controlo, mas não suportará necessariamente o sucesso organizacional [Galloway 1994].

O modelo COSO define o controlo interno como sendo um processo, constituído por cinco sub-processos, figura 3, desenvolvido para garantir, com razoável certeza, que sejam atingidos os objectivos perseguidos por uma organização, nas seguintes categorias: eficiência e efectividade operacional; confiança nos registos contabilísticos/financeiros e conformidade.

Entre Julho e Outubro de 2003 foi submetido à discussão pública o documento "*Enterprise Risk Management Framework*", pelo "*Committee of Sponsoring Organizations of the Treadway Commission"*.

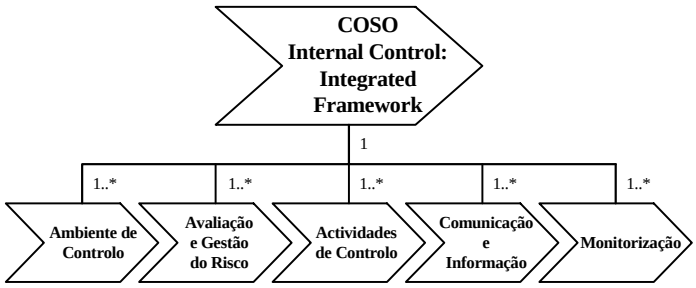

Figura 3 – O modelo de controlo interno "*Integrated Control: Integrated Framework*", proposto por "*the Comitee of Sponsoring Organizations*", é um processo constituído por cinco elementos.

5 A "FRAMEWORK" CEO E O CONTROLO INTERNO DE PROCESSOS DE NEGÓCIO

A FCEO, dotada com estereótipos adequados poderá suportar a modelação do controlo interno, simultaneamente com a modelação do negócio, garantindo a modelação de sistemas de controlo interno alinhados com o negócio.

Um mecanismo de controlo de um processo de negócio é um recurso consumido, usado, produzido ou refinado por um processo de controlo [modelo COSO, por exemplo]. Estes recursos devidamente relacionados com os processos de negócio, principais ou de suporte, dão garantia ao gestor da organização de atingir com razoável certeza os seus objectivos de negócio.

5.1 Extensão da "framework" CEO

Para que a FCEO possa suportar no seu metamodelo o modelo COSO de controlo interno, é necessário estender a sua notação.

Não existirá qualquer alteração aos objectos de negócio propostos na notação estudada por [Sinogas 2002], que continuarão a ser os objectivos, os processos, os recursos e os sistemas de informação.

Propõe-se que as classes predefinidas dos objectivos, processos e recursos sejam revistas e proposta a sua extensão, conforme se apresenta seguidamente, para poderem suportar a modelação do sistema de controlo interno.

1.5.1 Objectivos

Semântica

Os objectivos determinam e ***controlam*** o comportamento do negócio e revelam os estados desejáveis de alguns recursos do negócio.

Restrições

Cada objectivo deve corresponder no mínimo a um processo.

Notação Gráfica

A notação gráfica de objectivo usa o ícone descrito na figura 4 para representar o estereótipo objectivo <<goal>>.

Figura 4 – Notação gráfica de objectivo.

Classes Predefinidas

Um objectivo estratégico deve ser composto por objectivos operacionais e objectivos de controlo [Weigand and Moor 2001]. Os objectivos operacionais podem por sua vez ser especializados em objectivos quantitativos e objectivos qualitativos. Os objectivos de controlo podem ser especializados em objectivos específicos, figura 5.

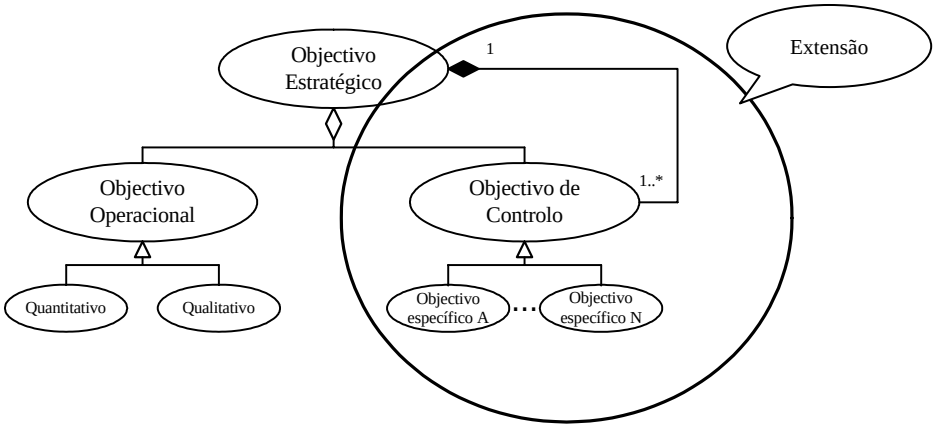

Figura 5 – Classes de objectivos predefinidas. Este modelo evoluiu relativamente ao proposto originalmente com a agregação e composição de um objectivo de controlo.

1.5.2 Processos

Semântica

Um processo representa uma unidade de trabalho, podendo a sua execução estar relacionada com a execução de outros processos através de fluxos de recursos. Um desses processos será certamente um processo de controlo.

Restrições

Um processo deve corresponder a um ou mais objectivos.

Notação Gráfica

A notação gráfica de processo usa o ícone descrito na figura 6 para representar o estereótipo de processo <<process>>.

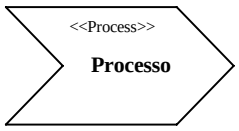

Figura 6 – Notação gráfica de processo.

Classes Predefinidas

As actividades de um negócio podem ser classificadas como actividades principais "*core*", actividades de suporte "*support*" e actividades de controlo "*control*".

As actividades principais e de suporte dependem do tipo de negócio que está a ser modelado podendo obviamente variar de organização para organização.

As actividades de controlo são as actividades necessárias para garantir que os processos principais ou de suporte são executados de acordo com as boas práticas. Estas actividades devem ter presente o suporte necessário à boa execução do processo de negócio, figura 7.

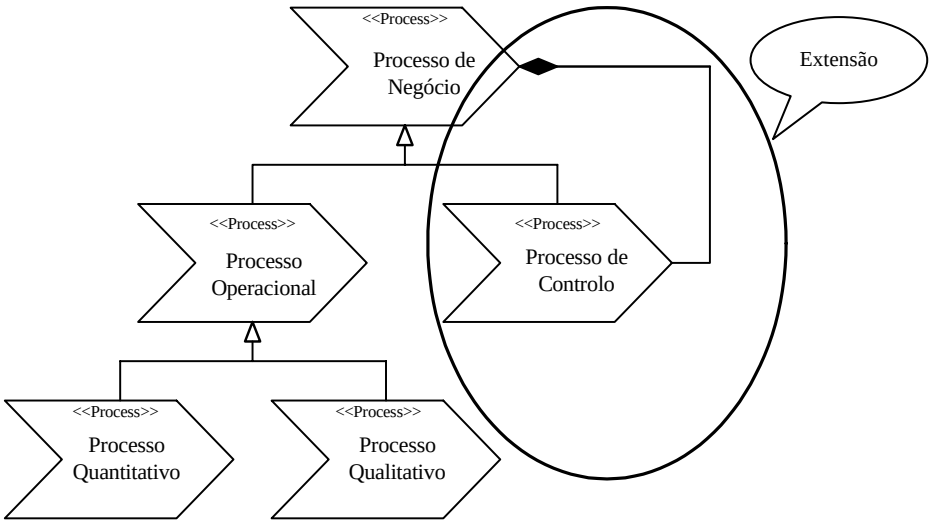

Figura 7 – Classes de processos predefinidas. Propomos que um processo de negócio seja especializado em processo operacional e processo de controlo, sendo este, sujeito simultaneamente a uma composição.

1.5.3 Recursos

Semântica

Os recursos são objectos do negócio que são manipulados através dos processos. Os recursos podem ser ordenados ou estruturados e ter relações entre eles.

Os recursos podem ser produzidos, consumidos, usados ou refinados pelos processos.

Restrições

Um recurso tem de ser produzido, consumido, usado ou refinado em pelo menos um processo.

Notação Gráfica

A notação gráfica para recurso usa o ícone mostrado na figura 8 para representar o estereótipo recurso <<resource>>.

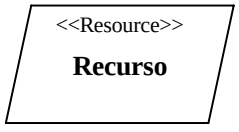

Figura 8 – Notação gráfica de recurso.

Classes Predefinidas

Os recursos de negócio de uma organização podem ser operacionais e de controlo. Os operacionais podem ser coisas ou informação e dividem-se em abstractos e físicos. Uma classe particular de recurso físico é pessoa ou entidade, figura 9.

Os recursos de controlo são definidos em função da análise de risco feita aos processos de negócio operacionais e aos sistemas que os suportam.

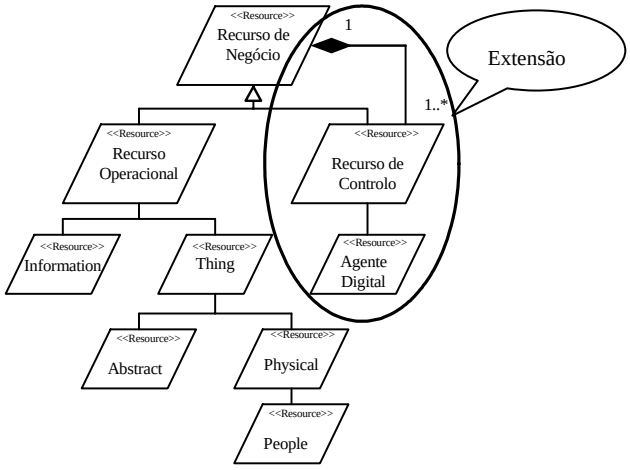

Figura 9 – Classes predefinidas de recursos.

1.5.4 Sistemas de Informação

No que respeita aos sistemas de informação não há qualquer proposta de extensão relativamente ao proposto por [Sinogas 2002].

5.2 Metamodelo da Evolução da FCEO

A figura 10 representa o metamodelo da evolução da FCEO. Pode verificar-se que a única alteração, relativamente ao metamodelo da FCEO original consiste na introdução da associação "*controls*" entre "*recurso*" e "*sistema*".

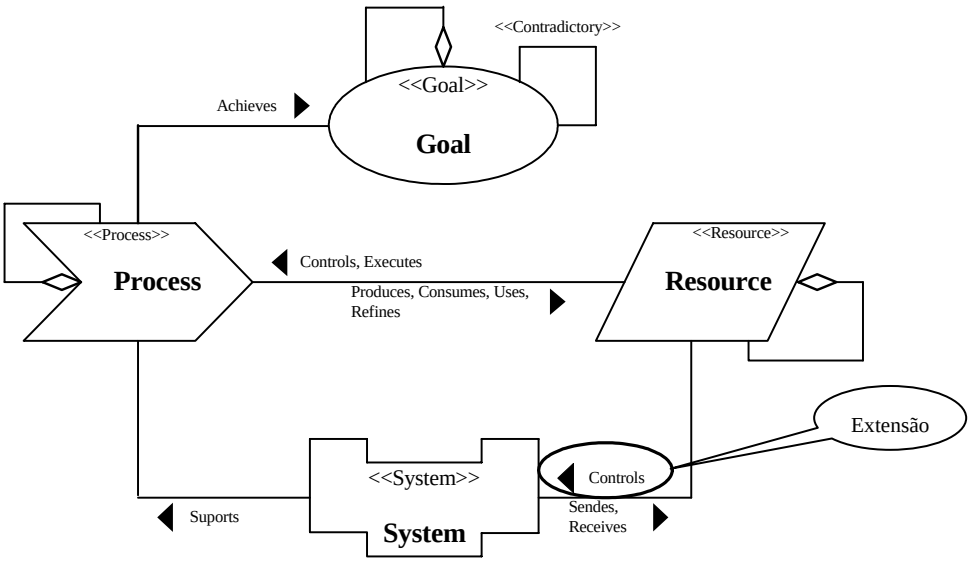

Figura 10 – Metamodelo da evolução da "framework" CEO. Verifica-se que o recurso pode passar a controlar os sistemas.

A tabela 1 apresenta de forma sistemática as restrições impostas pelo metamodelo acima às subclasses e objectos com os estereótipos definidos na "framework" CEO.

	Goal	Process	Resource	System
Goal	Contradicts			
Process	Achieves		Produces, Consumes, Uses, Refines	
Resource		Controls, Executes		**Controls**
System		Supports	Sends, Receives	

Extensão

Tabela 1 – Associações do metamodelo da evolução da "*framework*" CEO. Conforme se pode ver a evolução reside na generalização da associação "*controls*" entre *recurso* e *sistema*.

5.3 Modelação de um Processo de Negócio com o Controlo Associado

No contexto do presente trabalho consideramos o controlo como um recurso que é consumido pelos processos de negócio e sistemas de informação e que é produzido por um processo de controlo figura 11.

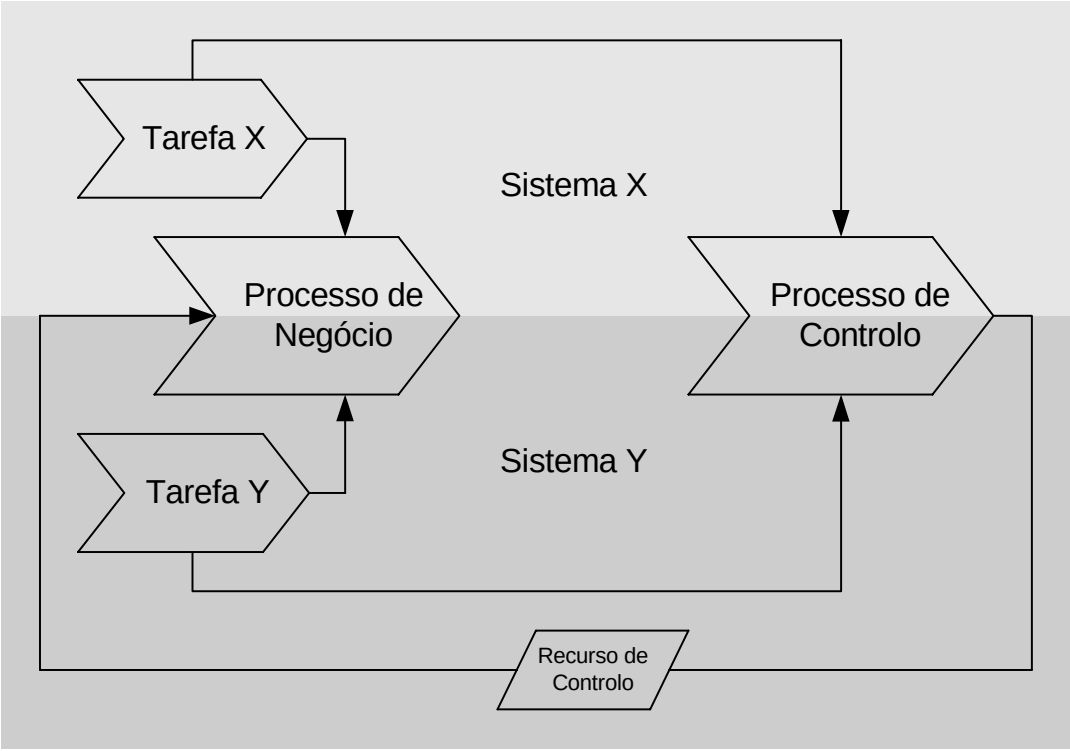

Figura 11 – Relação entre um processo de negócio e o processo de controlo associado.

Conforme referido na secção 5.1.1, associado aos objectivos operacionais de qualquer organização há sempre um objectivo de controlo [Weigand and Moor 2001]. Este objectivo deve garantir com razoável certeza que todos os objectivos operacionais são atingidos satisfatoriamente.

Por outro lado, para que se atinjam os objectivos de controlo específicos deve ser garantido que os processos que os suportam utilizam adequados recursos de controlo. Estes recursos são identificados em função do risco que se pretende minimizar ou mesmo eliminar figura 12.

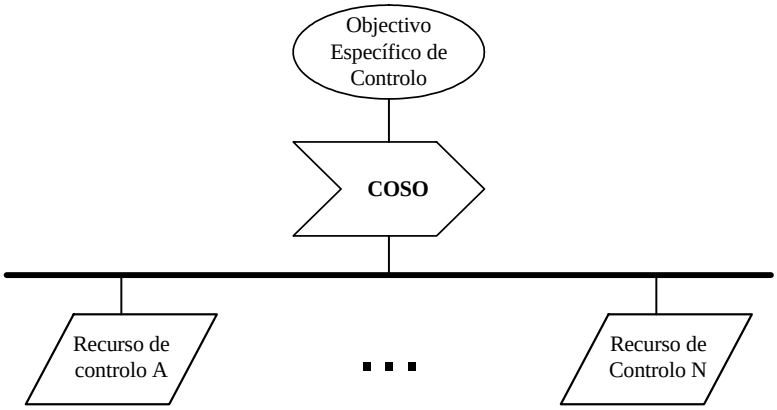

Figura 12 – Processo de controlo que consome ou produz recursos de controlo para todos os outros processos. Se se garantir que todas as actividades estão controladas os processos que as referidas actividades suportam estão igualmente controladas.

Para controlar este processo deverão ser seleccionados um ou mais pontos de controlo. Um ponto de controlo é qualquer pessoa, coisa, ou evento que em função das vulnerabilidades que apresenta deve ser sujeito a mecanismos de controlo para minimizar ou, se possível, anular o risco da eventual concretização da ameaça.

Relativamente aos pontos de controlo seleccionados podemos identificar algumas vulnerabilidades que podem ser exploradas por ameaças, a que possam estar sujeitos, podendo transformar-se em risco que é necessário, obviamente, minimizar, ou se possível anular.

As ameaças referidas potenciam um risco permanente que pode, na ausência de mecanismos de controlo, manifestar-se com efeitos perniciosos. Assim, é necessário minimizar a permanência desta ameaça, implementando adequados mecanismos de controlo. Isto é conseguido definindo um objectivo específico de controlo e identificando os adequados mecanismos de controlo, em função do referido objectivo, que minimizam a ameaça.

6 CONCLUSÕES

Confirmada a coerência da FCEO, requisito mínimo para poder suportar a modelação de mecanismos de controlo interno, estudámo-la na perspectiva do controlo interno. Este estudo deu indicações favoráveis à utilização da FCEO na modelação de mecanismos de controlo interno. Para o efeito verificou-se ser necessário propor ligeiras alterações ao seu metamodelo.

Com recurso à teoria do controlo interno e ao modelo COSO – "*Internal Control – Integrated Framework*" editado pelo "*Committee of Sponsoring Organizations of the Treadway Commission*", propomos a evolução da FCEO para que em qualquer processo de modelação de um negócio eventuais mecanismos de controlo sejam identificados, ou sejam possíveis as suas implementações. O metamodelo da FCEO estendida traduz-se em alterações mínimas ao metamodelo original da FCEO.

Finalmente, com a consciência de que o que aqui fica proposto é um modesto contributo, ainda havendo um longo caminho a percorrer para a modelação efectiva e coerente do controlo interno numa organização, propomos como trabalho futuro a utilização do metamodelo da FCEO estendida à modelação de processos de negócio, principais e de suporte, em situação real.

Fica ainda como proposta de trabalho futuro a investigação relacionada com a implementação ao nível dos sistemas de mecanismos de controlo que garantam o equilíbrio dos sistemas organizacionais.

7 REFERÊNCIAS

Aveiro, D. (2002). Organização da Função Informática. Instituto Superior Técnico. Lisboa, Universidade Técnica de Lisboa.

Castela, N. (2001). Recolha, Análise e Validação de Informação para Modelação de Processos de Negócio. Instituto Superior Técnico. Lisboa, Universidade Técnica de Lisboa.

Champlain, J. J. (1998). Auditing Information Systems: a comprehensive reference guide. New York, John Wiley & Sons, Inc.

Colbert, J. L. and P. L. Bowen, Eds. (2002). A Comparison of Internal Controls: COBIT, SAC, COSO and SAS 55/78, Information Systems Audit and Control Association.

Curtis, M. B. and F. H. Wu (2000). "The Components of a Comprehensive Framework of Internal Control." CPA Journal.

Galloway, D. J. (1994). Control Models in Perspective. The Internal Auditor. 51: pp. 46-52.

Hermanson, H. M. (2003). "COSO: More Relevante Now Than Ever." Internal Auditing 18(4): pp. 3-6.

Mendes, R. (2001). Modelação de Estratégia de Negócio: Representação, Alinhamento e Operacionalização. Instituto Superior Técnico. Lisboa, Universidade Técnica de Lisboa.

Moran, J. (2001). "Applying Best Practice Internal Control in the European Commission." Accountancy Ireland.

Namee, D. M. (1997). Risk-Based Auditing. Internal Auditor. 54: pp. 22-27.

O'Connel, P. (1999). Internal Control Standards.

Pathak, J. (2003). "Internal Audit E-Commerce Controls." Internal Auditing.

Sinogas, P. (2002). Modelação de Processos de Negócio. Instituto Superior Técnico. Lisboa, Universidade Técnica de Lisboa.

Vasconcelos, A. (2001). Arquitectura de Sistemas de Informação no Contexto do Negócio. Instituto Superior Técnico. Lisboa, Universidade Técnica de Lisboa.

Weigand, H. and A. d. Moor (2001). A Framework for the Normative Analysis of Workflow Loops. Sixth International Workshop on the Language-Action Perspective on Communication Modelling (LAP 2001), Montreal - Canada.