IV SINGEP
Simpósio Internacional de Gestão de Projetos, Inovação e Sustentabilidade
International Symposium on Project Management, Innovation and Sustainability
ISSN: 2317 - 8302

IT SOX FRAMEWORK – UM GUIA UTILIZADO PARA ORGANIZAR E AGILIZAR A COLETA DE EVIDÊNCIAS DE AUDITORIA SOX

SERGIO LUIS MATTOS MELCHIORI
UNINOVE – Universidade Nove de Julho
sergio_melchiori@hotmail.com

IV SINGEP
Simpósio Internacional de Gestão de Projetos, Inovação e Sustentabilidade
International Symposium on Project Management, Innovation and Sustainability
ISSN: 2317 - 8302

IT SOX FRAMEWORK – UM GUIA UTILIZADO PARA ORGANIZAR E AGILIZAR A COLETA DE EVIDÊNCIAS DE AUDITORIA SOX

Resumo

Devido a várias crises de credibilidade enfrentadas pelo mercado de capitais norte americano, foi necessário implantar uma nova legislação: Lei Sarbanex-Oxley ou SOX. Todas as empresas brasileiras com ações negociadas na bolsa norte-americana devem se adequar a esta lei. A adaptação a esta nova lei é bem onerosa para a empresa, porém se bem organizada pode gerar uma maior efetividade dos seus controles, bem como uma maior otimização dos recursos da empresa envolvidos no projeto. Por isso se fez necessário a criação do IT SOX Framework, que é um guia utilizado para organizar e agilizar a coleta de evidências da auditoria SOX. A metodologia utilizada foi a pesquisa-Ação onde o pesquisador interagiu com a equipe do projeto na busca da melhor forma de criar os procedimentos. Dentre outros benefícios, a implantação do IT SOX Framework reduziu o tempo e custo operacional, bem como melhorou a eficiência dos controles testados, comparando a auditoria anterior com a auditoria após a implantação do framework. A Lei Sarbabes-Oxley, apesar de custosa, pode trazer muitos benefícios à organização principalmente com relação a uma maior credibilidade dos investidores, por isso é importante que os gestores saibam utilizar os controles internos gerados em prol da empresa.

Palavras-chave: Sarbanex-Oxley, SOX, Auditoria, Controles internos, Governança.

Abstract

Due to various credibility crisis faced by the North American stock market, it was necessary to implement new legislation: Sarbanes-Oxley or SOX. All Brazilians companies with shares in North America stock market must adapt to this law. Adapting to this new law is very costly for the company, but if well organized can generate greater control effectiveness and optimization of resources involved in the project. Therefore, it was necessary to create the IT SOX Framework, which is a guide used to organize and speed up the collection of evidence of SOX audit. The methodology used was research-action in which the researcher interacted with the project team in finding the best way to create the procedures. Among other benefits, the implementation of IT SOX Framework has reduced the time and operating costs, and improved the efficiency of controls tested by comparing the previous audit with the audit after the implementation of the framework. The Sarbabes-Oxley, although costly, can bring many benefits to the organization mainly on the credibility of investors, so it is important that managers know how to use internal controls in favor of the company.

Keywords: Sarbanex-Oxley, SOX, Audit, Internal control, Governance.

ISSN: 2317 - 8302

1 Introdução

A auditoria é uma importante ferramenta para mitigar inúmeros riscos, erros e desperdícios dentro de uma organização. Por meio da auditoria, é possível verificar se todos os processos internos e políticas definidas pela companhia estão sendo efetivamente seguidas. Existem dois tipos de auditoria: Auditoria Interna e Externa. A auditoria interna, surgiu com a expansão dos negócios e consequentemente de dar maior foco às normas e procedimentos internos. Já a auditoria externa, realizada por uma empresa independente, não elimina a necessidade de uma auditoria interna, visto que esta última permite a identificação e resolução antecipada de problemas antes da chegada da auditoria externa.
A auditoria surgiu com a necessidade por partes dos investidores e proprietários de confrontar os valores retratados no patrimônio, provendo desta forma, maior confiança para os proprietários que os procedimentos estão sendo seguidos conforme planejados e maior credibilidade para os investidores acreditarem na empresa da qual estarão depositando seu capital.
Apesar das auditorias externas, na década de 90 o cenário econômico dos Estados Unidos estava em crise, devido ao mercado de capitais que se encontrava abalado em decorrência dos graves escândalos contábeis envolvendo empresas como Enron e WorldCom (SANTOS & LEMES, 2004), onde estas "maquiavam" seus balaços patrimoniais com anuência da auditoria externa. Autoridades norte-americanas foram unânimes em aprovar uma nova legislação: a Lei Sarbanex-Oxley ou SOx. Esta lei é considerada uma das mais rigorosas regulamentações ao se tratar de controles internos, elaboração de relatórios financeiros e divulgação, já aplicadas. Esta lei aplica-se as organizações abertas norte-americanas e estrangeiras que tenham ações negociadas no mercado americano.

1.1 A situação problema

Devido à grande importância desta auditoria nas organizações, se faz necessário a criação de um procedimento efetivo e estruturado de coleta de evidências. O Estudo apresentado neste relato é referente uma empresa multinacional do ramo de seguros que possui capital negociado no mercado americano e por isso sujeito a legislação da Lei Sarbanex-Oxley. Nesta empresa, a coleta de evidências era feita de forma reativa, ou seja, apenas quando se iniciava uma auditoria, uma equipe era mobilizada para fazer a coleta de evidências. Antes da implantação do framework este trabalho era feito de forma desestruturada, onde profissionais eram retirados dos projetos em curso e alocados na auditoria, muitas vezes tendo que atuar nos dois projetos ao mesmo tempo. Além disso, se o profissional não tivesse o conhecimento prévio de como se extraia uma evidência específica, o tempo dispensado para este trabalho poderia aumentar substancialmente devido a falta de documentação existente.
A solução para esta problemática foi transformar a coleta de evidências de uma forma reativa, para uma forma proativa, de uma estrutura desorganizada para uma organizada, além de gerar métricas de maturidade para cada controle de auditoria e desta forma permitir uma visão holística de todo o cenário da auditoria. A ideia para solucionar este problema foi a criação do SOX IT Framework, documentação que especifica em detalhes o que deve ser feito, quando deverá ser feito, como fazer, quem é o responsável e onde deverá ser armazenada as evidências coletadas. Além disso, o framework medirá o nível de maturidade de cada controle SOX no momento atual e sua evolução com o tempo, com as seguintes métricas de controle: Pendente, Inexistente, Definido, Repetido, Gerenciado e Otimizado.

O objetivo deste trabalho é atingir um maior nível de maturidade nos controles da auditoria SOX, diminuir o número de controles ineficientes, além de diminuir substancialmente o tempo gasto da equipe dispensado à auditoria, gerando desta forma uma economia para a empresa. Para isto, foram medidos os tempos de execução da coleta e a efetividade dos controles da auditoria anterior, contra a auditoria realizada após a implantação do SOX IT Framework.

2 Referencial Teórico

Cada vez é maior a preocupação de governo, acionistas e outros interessados com a credibilidade das informações geradas pelas empresas, visto que envolvem grandes valores monetários. Casos de escândalos financeiros acontecidos nos Estados Unidos reforçam ainda mais toda esta preocupação. Casos notórios de empresas como Enron, Tyco e WordCom são exemplos de desastres que afetaram a credibilidade do sistema financeiro mundial, segundo (Shehade, Lopes, & Conter, 2013).

Esta série de escândalos motivou as autoridades reguladoras a promulgar a lei Sarbanex-Oxley (Sox). Segundo a Wikipédia: "A lei Sarbanes-Oxley, apelidada de Sarbox ou ainda de SOX, visa garantir a criação de mecanismos de auditoria e segurança confiáveis nas empresas, incluindo ainda regras para a criação de comitês encarregados de supervisionar suas atividades e operações, de modo a mitigar riscos aos negócios, evitar a ocorrência de fraudes ou assegurar que haja meios de identificá-las quando ocorrem, garantindo a transparência na gestão das empresas." Esta lei estabeleceu severas regras às pessoas envolvidas nas organizações incluindo: administradores, auditores, advogados, analistas de mercado, diretores entre outros (de Oliveira, 2006).

Os efeitos da lei Sabanex-Oxley são muito significativos tanto nos Estados Unidos como em todo o mundo, uma vez que as empresas passaram a ter que se adaptar a um cenário de mudanças, principalmente com relação a auditoria interna, onde é necessário ter uma definição clara e detalhada dos controles de cada área, para que desta forma, pudessem passar de forma transparente aos administradores e investidores a situação patrimonial e financeira da empresa.(da Silva & Machado, 2010).

De acordo com (Silva 2007) apud (da Silva & Machado, 2010), as penalidades pelo descumprimento da SOX são: certificação de qualquer documento em desacordo com as exigências estipuladas: US$ 1.000.000,00 (um milhão de dólares americanos), ou a reclusão por 10 anos, ou ambos e pela certificação, internacional, de qualquer demonstrativo em desacordo com as exigências estipuladas: US$ 5.000.000,00 ou a reclusão por 20 anos, ou ambos.

A SOX obrigou as empresas na adoção de várias práticas e novos controles, com o objetivo de garantir a exatidão, confiabilidade e transparência na divulgação das informações financeiras e administrativos. Apesar da rigidez dos controles, a organização pode se beneficiar deles se souber utilizá-los, destacando entre eles, a chance de obter informações mais pontuais, tomada de melhores decisões operacionais, conquista da confiança dos investidores e ainda melhor vantagem competitiva através de operações dinâmicas segundo (Shehade et al., 2013).

Dentre os principais impactos da SOX que as empresas tiveram destacam-se: a criação da área de auditoria interna, devido ao grau de detalhamento dos controles, grau de responsabilidade dos altos gestores e executivos e mais transparência nos relatórios financeiros. Dentre as principais mudanças ocorridas nas empresas, destacam-se os gastos referentes a implantação dos processos de auditoria baseados na SOX, com consultoria devido à complexidade das informações, contratações de novos funcionários, maior número de controles SOX para a equipe suportar segundo (da Silva & Machado, 2010).

3 Metodologia

O método da Pesquisa-Ação foi escolhido para a realização deste trabalho, neste sentido, os atores participaram junto com o pesquisador, interagindo na busca da melhor forma de executar e sanar a problemática da pesquisa. A pesquisa-Ação, segundo (Thiollent 1997), possui uma rotina compostas por três principais ações que são: Observar, com o intuito de coletar informações e criar um novo cenário. Pensar, com o intuito de explorar, analisar e interpretar os fatos e agir, com o objetivo de implementar e avaliar as ações. Segundo a literatura de Thiollent, o processo de pesquisa-Ação é dividido em 4 fases:

1) Fase exploratória: Foram analisados os resultados finais das auditorias SOX do ano anterior, analisados os controles que mais falhavam através de relatórios gerados após a auditoria. Além disso, foram coletadas atas de reuniões com a equipe do projeto, bem como as documentações de recomendações de melhorias sugeridas pelos auditores.

2) Fase de pesquisa aprofundada: nesta fase foi feita uma análise aprofundada de toda documentação coletada na fase anterior, e notou-se que a cada nova auditoria, uma pessoa da equipe era designada para coletar as evidências dos controles, porém não existia nada documentado em nenhum lugar, como estes controles eram extraídos para serem enviados para os auditores, não havia exemplos dos controles dos anos passados, que poderiam servir como base para os anos seguintes. Por isso, todo *expertise* conquistado em uma auditoria era dissipado nos anos posteriores, causando um enorme retrabalho e um maior esforço da equipe. Além de todo o retrabalho, controles que já tinham sido regularizados eram apontados como falhos nos anos seguintes por falta de conhecimento do funcionário em saber quais eram os passos para extrair de forma correta determinado controle, causando grande desconforto na equipe e uma perplexidade na equipe do projeto. Desta forma, foi proposto a criação de um framework de controle SOX. Este framework teria como objetivo principal documentar as informações relativas a cada controle da auditoria, criação de um repositório único de armazenamento das evidências, procedimentos para extração das evidências, criação de matriz de responsabilidades, para que cada funcionário saiba seu papel em cada controle, elaboração de um controle de frequência dos controles, ou seja, o funcionário saberia de antemão quando teria que se dedicar à auditoria, dando a chance para o mesmo de organizar suas atividades do dia a dia, além de propor níveis de maturidade de cada controle e ainda acompanhar sua evolução durante os anos. Outro aspecto muito importante neste framework é que se um funcionário sair de sua função, o conhecimento não se perde e desta forma uma outra pessoa poderia ocupar o lugar deste empregado sem que o conhecimento se perdesse.

3) Fase de Ação: Foi criado um Framework e batizado com o nome de IT SOX Framework, com o apoio de toda a equipe do projeto. A implementação deste se iniciou no mês de julho de 2015 e foi concluído no mês de agosto de 2015. Os atores e pesquisadores trabalharam lado a lado na criação deste framework.

4) Fase de avaliação: nesta fase foi medido o novo tempo gasto para se coletar as evidências. A diferença do tempo anterior para o atual, multiplicado pelo valor hora do funcionário, é o valor da economia da empresa adotando este framework. Também foi medido o número de controles efetivos, comparando os controles dos anos anteriores com os controles do ano atual.

4 Tipo de Intervenção

ISSN: 2317 - 8302

A intervenção realizada em campo juntamente com a equipe do projeto, foi a criação do IT SOX Framework, que contempla as informações pertinentes a auditoria SOX, que serão descritas a seguir.

4.1 Escopo da Auditoria

A auditoria pode coletar evidências de diversos setores de uma empresa, como no departamento de recursos humanos, departamento financeiro entre outros.
Este relato trata da coleta de evidências designadas ao departamento de tecnologia da informação (TI). A auditoria SOX solicita para a área de TI extrair evidências dos seguintes controles a seguir.
Para cada controle abaixo uma evidência deve ser extraída e enviada ao auditor.
A tabela a seguir representa todo os controles solicitados pela auditoria SOX.

Controle de Auditoria SOX
(T1) 01.01.01.04 - Periodicamente revisar os acessos dos funcionários de TI e a autorização apropriada para acesso ao sistema. Incluindo a revisão das funções atribuídas aos usuários e a tomada de ação apropriada identificada na revisão.
(T5) 01.01.03.01 - Documentar e revisar periodicamente as políticas e procedimentos chaves requeridos para o mínimo controle geral de TI.
(T7) 01.02.01.03 - Logar e resolver problemas operacionais de TI e problemas em produção.
(T8) 01.02.02.02 - Acesso restrito para modificar job schedules para indivíduos autorizados.
(T9) 01.02.02.04 - Logar e resolver processos de Job scheduling ou processamento de problemas de tarefas.
(T10) 01.02.02.05 - Documentar e obter autorização apropriada para alteração de job schedules.
(T15) 01.03.01.01 - Implementar e aderir a uma metodologia de desenvolvimento de sistemas documentada, para novas implementações e alterações significantes que incluem testes e aprovação de mudanças.
(T17) 01.03.02.03 - Implementar e aderir a um processo de controle de mudanças documentado para alterações nas aplicações que incluem testes e mudanças aprovadas.
(T18) 01.03.02.04 - Acesso restrito para implementar mudanças para indivíduos autorizados.
(T19) 01.03.04.01 - Implementar e aderir um controle de mudança de processo de infraestrutura que inclui teste e mudanças aprovadas.
(T20a) 01.04.01.01 - Documentar e obter a apropriada autorização do time de negócios, para contas novas e modificas. Autorização inclui assinatura da pessoa responsável.
(T20b) 01.04.01.01 - No mínimo anualmente, ou mais frequente quanto possível, a lista de gerentes autorizadores com a função de aprovar acessos de usuários novos e modificados é revisada e atualizada para mudanças da organização. A lista pode ser mantida manualmente ou no sistema.
(T21a) 01.04.01.02 - Existir um controle para garantir que o time de negócios notifica o adminitrador da aplicação com relação aos transferidos e demitidos.
(T21b) 01.04.01.02 - O departamento de TI toma ação apropriada no tempo adequado após o recebimento da notificação dos transferidos e demitidos.
(T22) 01.04.01.03 - O acesso do usuário é concedido via usuário de conta individual (não genérico/contas compartilhadas) e documentar e obter a apropriada autorização para as exceções.
(T23) 01.04.01.05 - Forçar alteração de password nos sistemas dentro de 91 dias.
(T24) 01.04.01.06 - Forçar um número mínimo de caracteres (8 caracteres por sistema).
(T25) 01.04.01.07 - Forçar um número limitado de logins inválidos para usuários antes da conta ser blooqueada pelo sistema.
(T26) 01.04.01.08 - Desabilitar/Remover ou mudança de senhas a cada 91 dias para contas default.

(T27) 01.04.02.01 - Periodicamente revisar usuários administradores e outras contas de usuários privilegiados e suas respectivas autorizações para acesso ao sistema. Incluindo revisão de assinatura dos gerentes e tomada de ações identificadas na revisão.
(T28) 01.04.02.02 - Periodicamente alterar as contas administrativas e outras senhas de contas privilegiadas nas demissões ou mudancas de funções de funcionários.
(T29) 01.04.03.02 - Periodicamente revisar os administradores de banco de dados e acesso de outras contas privilegiadas e suas respectivas autorizações de acesso ao sistema. Incluindo revisão de assinatura dos gerentes e tomada de ações identificadas pela revisão.
(T30) 01.04.03.03 - Desabilitar/remover or alterar senha a cada 91 dias para as contas default do banco de dados.
(T37) 01.04.05.02 - Documentar e obter autorização apropriada para o acesso físico ao data center(s).
(T39) 01.04.05.04 - Periodicamente revisar o acesso físico ao data center(s).
(T40) 01.06.01.02 - Implementar e aderir a ferramentas/procedimentos que assegure que os backus sejam completados com sucesso.
(T41) 01.06.01.03 - Logar e resolver problemas de backup.

Figura 1. Controles de Auditoria Sox

O Framework, para uma melhor visualização, agrupou os controles da auditoria em: 1. Data Centers (DC) 2. Firewalls (FW) 3. Domínio/Redes (DO) 4. Servidores (SE) 5. Aplicações (AP) 6. Base de dados (BD).
Para cada agrupamento apresentado acima, podemos ter um ou mais controles, ou seja, para o agrupamento Base de Dados (BD), poderemos ter controles a respeito de *Jobs*, *Backups* entre outros. Cada controle é representado pela sigla do agrupamento DB, seguido do número do controle.

4.2 Níveis de Maturidade

Ao final de cada auditoria, é atribuído a cada controle um nível de maturidade, conforme mostra o quadro a seguir:

Nível de Maturidade	Descrição
4 - Otimizado	**Eficiência da evidência do processo comprovada mais de uma vez pela auditoria externa.**
3 - Gerenciado	**Eficiência da evidência do processo comprovada pela auditoria externa.**
2 - Repetido	**Eficiência da evidência do processo comprovada pela auditoria interna.**
1 - Definido	**Procedimento de extração da evidência existente, porém ainda não foi comprovado em uma auditoria.**
0 - Inexistente	**Procedimento de extração da evidência inexistente.**
-1 - Pendente	**Processo inefetivo na auditoria interna ou externa**

Figura 2. Níveis de Maturidade

-1 – Pendente: O nível "-1" demostra que o controle falhou na auditoria, seja ela uma auditoria interna ou externa.
0 – Inexistente: Quando o nível de maturidade do controle é igual a zero, significa que o controle é novo e por isso não existem procedimento de extração da evidência. Obs.:

ISSN: 2317 - 8302

Acontece nas auditorias, principalmente nas externas, dos auditores solicitarem novos controles, nestes casos o nível de maturidade é zero.

1 – Definido: Quando o controle possui este nível, significa que já foi executado internamente, porém ainda não foi testado em nenhuma auditoria, seja ela interna ou externa.

2 – Repetido: Neste estágio, o controle já passou por uma auditoria interna pelo menos e foi efetivo.

3 – Gerenciado: Neste estágio, o controle já passou por uma auditoria externa pelo menos e foi efetivo.

4 – Otimizado: Este é o nível mais alto de maturidade. Ao ser atribuído este nível, o controle já passou e foi efetivo em mais de uma auditoria externa.

4.3 Mapa de Modelo de Maturidade

Para cada um dos agrupamentos: DC, FW, DO, SE, AP e BD, um mapa de maturidade será criado com todos os seus respectivos controles.

A figura a seguir, mostra um exemplo do mapa de maturidade do agrupamento DC que possui cinco controles: DC1, DC2, DC3, DC4 e DC5.

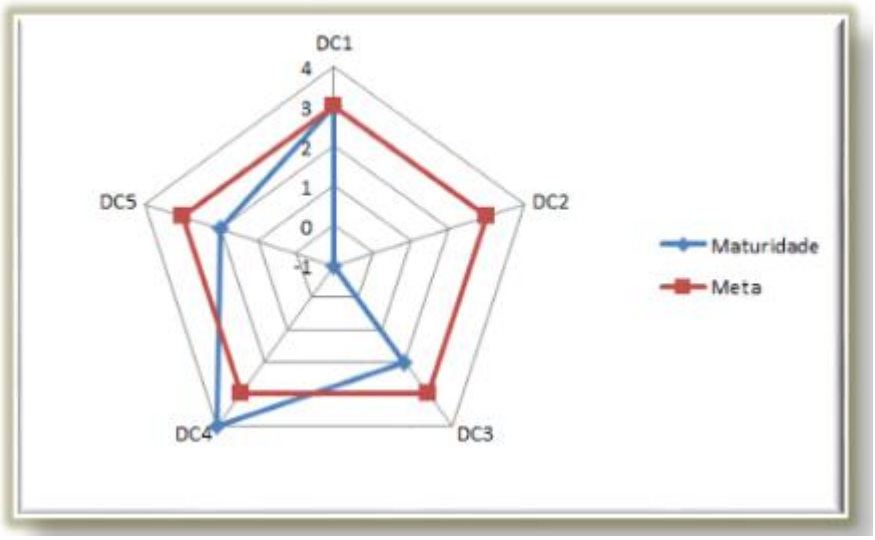

Figura 3. Mapa do Modelo de Maturidade

A Figura 3 mostra os cinco controles do agrupamento Data Center (DC). A linha azul mostra o nível de maturidade de cada controle. O controle DC1 tem o nível de maturidade 3, o controle DC2 tem o nível de maturidade -1, o DC3 tem o nível de maturidade 2, o DC4 tem nível de maturidade 4 e finalmente o controle DC5 tem nível de maturidade 2.

A linha vermelha mostra a meta esperada para cada controle, no exemplo acima o gestor estipulou o nível 3 como um nível satisfatório para cada controle.

4.4 Mapa de Controle de Auditoria

O mapa de controle de auditoria foi criado para registrar todas as auditorias realizadas, bem como as auditorias previstas. Desta forma os recursos podem se programar para a data da realização da coleta das informações.

Para cada auditoria é gerado um código sequenciador. Além deste código é informado a descrição da auditoria, o período que se coletou as evidências (De – Até) e a data da realização da auditoria.

Cód Auditoria	Descrição da Auditoria	Data Inicial
01	Auditoria Interna SOX	01/07/2013
02	Auditoria Externa SOX	10/09/2013
03	Auditoria IBM	01/01/2014
04	Auditoria Interna Affinity	01/01/2015
05	Auditoria Interna SOX	01/07/2015

Figura 4. Mapa do Controle de Auditoria

4.4 Mapa de Evolução dos Controles de Auditoria

Este artefato foi criado para verificar não apenas o nível de maturidade atual de cada controle, como sua evolução com o tempo.

Data Center	Dono do Processo	Cód. 01	Cód. 02	Cód. 03	Cód. 04
DC1	Fulano 1	3	3	3	
DC2	Fulano 1	1	1	2	
DC3	Fulano 2	1	1	2	
DC4	Fulano 2	1	1	2	
DC5	Fulano 2	4	4	-1	

Figura 5. Mapa de Evolução dos Controles

Conforme mostra a Figura 5, na primeira coluna (Data Center) são descritos os controles do agrupamento Data Center. Para cada controle, um dono é designado e informado na coluna (Dono do Processo). As colunas subsequentes (Cod. 01, Cod 02, Cod. 03 e Cod. 04) são referentes aos códigos das auditorias. Os números, abaixo das colunas de códigos, representam a evolução do nível de maturidade dos controles, de acordo com a sequência de auditorias. As cores representam se o controle foi efetivo (verde), se o controle ficou pendente (amarelo) ou se o controle foi não efetivo (vermelho).
Obs.: Um controle pode ser considerado pendente quando o mesmo poderá ser testado em uma próxima auditoria.

4.5 Framework

O IT SOX Framework foi construído com as seguintes informações:

Descrição de todos os controles: Conforme Figura 1 – Controles de auditoria sox. **Dono de cada controle:** Pessoa responsável da equipe em gerar a evidência e garantir a efetividade do controle. **Frequência de cada controle**: Informação se o controle é semestral, anual ou outros. **Papeis e responsabilidades de cada controle**: Além do dono do controle, outras

pessoas podem ficar responsáveis pela extração de parte da evidência, por isso para cada controle foi criado uma matriz de responsabilidades. **Procedimento de geração de cada controle**: Para cada controle será descrito o procedimento, passo a passo, de como cada evidência é gerada, para que outra pessoa lendo os procedimentos possa, da mesma forma, extrair a evidência do controle. **Local de armazenamento de cada controle**: No framework será informado o local de armazenamento das evidências de cada controle. **Referência de cada controle**: Neste campo será informado de qual auditoria o controle se refere, se uma auditoria interna ou uma auditoria externa. **Histórico de alterações de cada controle**: Se houve alguma alteração na descrição do controle de um ano para o outro, será informado neste campo. **Nível de maturidade de cada processo**: Conforme Figura 2, será atribuído um nível de maturidade para cada controle. **Mapa de controle de auditoria**: Conforme Figura 4 - – Mapa de Controle de Auditoria. **Mapa de evolução de controles**: Conforme item 5 – Mapa de Evolução de Controles. **Mapa do modelo de maturidade**: Conforme Figura 3 – Mapa do Modelo de Maturidade.

5 Apresentação e Análise dos Resultados

A criação do SOX IT Framework trouxe vários benefícios para a empresa em questão, organizou todas evidências em um único local, onde o recurso poderá encontrar facilmente qualquer evidência de qualquer ano. Outro ponto importante a ser destacado é que como o procedimento de extração da evidência é muito detalhado, este fica com uma complexidade mais baixa, diminuindo o retrabalho e permitindo que recursos de cargos e salários mais baixos possam executar as tarefas. E finalmente, o SOX IT Framework permitiu a equipe do projeto, bem como a direção da empresa, ter uma visão holística da situação de todos os controles sox, tanto na visão atual, como em sua evolução do nível de maturidade de todos os controles.

Para apresentação dos resultados de melhorias com relação a implantação do IT SOX Framework, foram comparados dois fatores entre a auditoria do ano passado, e auditoria deste ano.

O primeiro fator foi o tempo que consequentemente afeta o custo do projeto. No ano passado os seis recursos do projeto levaram quatro semanas para finalizar a extração de todas as evidências, enquanto que este ano, os mesmos seis recursos extraiam todas as evidências em três semanas, gerando uma economia de 25% do tempo da equipe do projeto.

O segundo fator é a efetividade nos controles gerados após a criação do Framework.

No ano passado, os seguintes controles falharam na auditoria T9, T5, T21a, T21b, T30 e T41.

Neste ano nenhum controle falhou, o que representa 100% dos controles efetivos.

6 Conclusão

A lei Sarbanex-Oxley estabelece um novo patamar de governança corporativa, criando rigorosas exigências sobre os controles e aumentando o grau de responsabilidade da alta gestão pelos relatórios financeiros gerados (Shehade et al., 2013).

Apesar de custosa, é importante que a gestão da empresa saiba fazer com que a adequação às leis gere valores para a organização, proporcionando melhorias nos processos internos da empresa, bem como maiores ganhos financeiros e qualidade operacional. (de Oliveira, 2006).

Este estudo propôs a melhoria dos processos internos de auditoria com o intuito de agilizar a coleta de evidências solicitadas na auditoria, bem como a otimização de recursos do projeto gerando ganhos financeiros. O relato também mostrou que a implantação do framework gerou

outros benefícios que não puderam ser medidos, como a criação de documentação de todas as evidências para se ter como referência para os anos seguintes, diminuição da complexidade da extração das evidências e redução de retrabalho devido as informações organizadas no framework. Além disso, permitiu uma visão holística da alta gestão dos controles de auditoria. Este estudo também mostrou uma economia de 25%, comparado como o ano anterior, com relação ao tempo da equipe do projeto após a implantação do framework. Outro fator importante foi a redução de seis controles não efetivos para nenhum controle não efetivo.

7 Referências

da Silva, L. M., & Machado, S. de B. Z. . (2010). UM ESTUDO SOBRE OS IMPACTOS DA LEI SARBANES–OXLEY NA ÁREA DE AUDITORIA INTERNA DE UMA EMPRESA BRASILEIRA COM AÇÕES NEGOCIADAS NOS ESTADOS UNIDOS. Setembro 7, 2015, de fapanpr Web site: http://www.fapanpr.edu.br/site/docente/arquivos/ARTIGO%2001.pdf

de Oliveira, R. V.. (2006). A Lei de Sarbanes-Oxley como nova motivação para mapeamento de processos nas organizações. Setembro 7, 2015, de Enegep Web site: http://www.abepro.org.br/biblioteca/enegep2006_tr450313_8769.pdf.

SANTOS, L. de A. A., & LEMES, S. (2004). A Lei Sarbanes-Oxley: uma tentativa de recuperar a credibilidade do mercado de capitais norte-americano. In *Congresso USP de Controladoria e Contabilidade, 4º, São Paulo. Anais. FEA/USP*.

Shehade, T., Lopes, S. A., & Conter, A.. (2013). Impacto dos controles SOX em Governança de TI. Julho 5, 2015, de Seicom Web site: http://www.udc.edu.br/v4/nucleodepaginas/producoes_partesEspecificas/SEICOM2014/files/07b.pdf

THIOLLENT, M. Pesquisa-Ação nas Organizações. Ed. Atlas. São Paulo, 1997.