Resenha do livro

Sarbanes-Oxley – Conforrmidade TI usando COBIT e ferramentas open source

Referência Bibliográfica

LAHTI, Christian e RODERICK, Peterson. Sarbanes-Oxley – Conforrmidade TI usando COBIT e ferramentas open source. Rio de Janeiro: Starlin, 284 p.

1. Principais Frases e Palavras-Chave relacionadas à disciplina FNSI

"Ato Sarbanes-Oxley", "COBIT", "dominios", "risco", "ferramentas e aplicativos", "monitoração", "PDCA", "open source", "Gnu", "Free software foundation", "ROI", "custos", "fluxo de trabalho", "SAS-70", "CIO", "CFO", "CEO", "políticas de segurança".

2. Principais Definições e Conceitos Úteis à disciplina FNSI

"COBIT significa Control Objectives for Information and Related Technology. Embota exista desde 1996, as diretrizes e praticas quase se tornaram o padrão de fato para auditores e a conformidade SOX, em grande parte porque os padrões COBIT são independentes da plataforma."

"Há aproximadamente 300 objetivos genéricos COBIT agrupados sob seis componentes. Ao examinar e aplicar as diretrizes e praticas COBIT, lembre-se de que elas terão de ser personalizadas de acordo com seu ambiente especifico."

"Você deve avaliar suas necessidades e prioridades individuais ao tomar a decisão de reposicionar seu departamento de TI. Se aceitar esse desafio, console-se em saber que a maioria das atividades de reposicionamento que terá de executar são as mesmas necessárias à obtenção da conformidades SOX."

"Faça da maneira mais difícil! Pense em seu trabalho antecipadamente. Dessa forma, nada no mundo poderá mantê-lo fora do alcance. Faça-o melhor do que precisa ser feito. Da próxima vez que o fizer será brincadeira de criança. Não deixe nada nem ninguém ficar entre você e a tarefa mais difícil, não deixe que nada impeça essa grande chance de ganhar força através da adversidade, confiança através do domínio, sucesso através do merecimento. Faça sempre melhor. Faça melhor do que qualquer outra pessoa faria. Sei que isso soa antiquado. E realmente é, mas o mundo foi construído assim." – Harlow H. Crutice, presidente da General Motors de 1953 e 1958.

"Deming desenvolveu um diagrama usando quatro setas em um padrão cíclico. Normalmente esse diagrama é conhecido como PDCA" – ref. Ciclo PDCA de W.Edwards Deming da década de 50.

3. Importância da leitura, análise e compreensão do livro / lei para MBIS Segurança da Informação

Este livro tem como objetivo trazer à tona as necessidades inerentes a todas as empresas de controle e preparação do departamento de TI para conformidade SOX, tendo como foco principal para o mesmo COBIT, onde demonstra dentro de seus objetivos a aplicabilidade em qualquer segmento de negocio. Os autores também demonstram o uso de ferramentas open source para cada um dos quatro domínios estruturais COBIT (Planejamento e Organização/ Aquisição e implementação/ Distribuição e suporte/ Monitoração e avaliação).

Um ponto muito importante a ser sempre considerado, são as conseqüências da não adequação a auditoria SOX, como multa e reclusão, no caso de a empresa não atender a conformidade.

Em todo o contexto do livro, muitas são as referencias quanto ao "PDCA" onde em cada um dos domínios apresentados, referencia-se também fazes de planejamento, execução, checagem e ações corretivas para que todos os componentes estejam fundamentados e resguardados de forma lógica.

É muito importante lembrar que todos os componentes COBIT, e por sua vez seus objetivos possuem uma carga generosa de documentos e normas a serem seguidas, sendo o mesmo não somente um processo a ser adotado, mas sim um conjunto de componentes e normas a serem seguidas durante toda a vida da empresa, podendo tornar o departamento de TI, de uma mera ferramenta de reparo de equipamentos da empresa a um departamento estratégico da empresa, trabalhando em conjunto com os demais (CFOs, CEOs e controladoria da empresa) no objetivo de que o ROI(returno on investment) seja efetivo.

Conforme a seção 404 do ato Sarbanes-Oxley que determina uma avaliação anual dos controles e procedimentos internos para emissão de relatórios financeiros. Além disso, o auditor independente da companhia deve emitir um relatório distinto, que ateste a veracidade de informações da administração sobre a eficácia dos controles internos e dos procedimentos executados para a emissão dos relatórios financeiros. Que por sua vez incorre nos princípios básicos da segurança da informação (Disponibilidade, Confidencialidade e Integridade).