CLEBERMARQUES
WWW.CLEBERMARQUES.COM

Microsoft®
Operations Framework 4.0
Simplificando o Gerenciamento de Serviços de TI

SMF Governance, Risk, and Compliance (GRC)

Governança, Risco e Conformidade

Última revisão feita em 22 de Dezembro de 2008.

Objetivo

Este artigo introduz a primeira SMF da camada Gerenciar, nós veremos as atividades que fazem parte da função GRC e também os procedimentos que devem ser executados para alcançarmos os objetivos definidos aqui. Tenha uma ótima leitura.

Obs.: As informações deste artigo são básicas e destinadas ao prévio entendimento do MOF 4, para maiores detalhes acompanhe a série de vídeos no site do Projeto MOF Brasil.

Introdução

Todos os colaboradores em uma organização devem compartilhar um entendimento comum quando se trata de Governança, Riscos e Conformidade. Governança é uma atividade gerencial que deixa mais claras as tomadas de decisão determinando responsabilidades para gerar resultados e endereçar avaliação de desempenho, trazendo transparência para a área de TI. Riscos representam possíveis impactos derivados de ações feitas ou não feitas, conformidade é uma atividade que assegura que pessoas estão seguindo regras, políticas e procedimentos definidos pela organização. A SMF GRC (Governance, Risk and Compliance) justificará porque estas atividades devem ser tratadas juntas e mostrará as atividades necessárias para se realizar cada tarefa.

Figura 1 – A SMF GRC no MOF 4.0.

Objetivos

Um dos principais objetivos desta SMF é possibilitar o oferecimento de serviços de TI efetivos, eficazes e em conformidade com políticas, leis e regulamentações, estabelecendo uma tomada de decisão clara e gerenciando riscos da melhor forma possível.

Processos

Para que cada um dos processos desta SMF seja realizado existe um fluxo, este fluxo pode acontecer de forma seqüencial ou paralela, dependendo de como cada processo funciona dentro da organização. É claro que quando existem dependências entre um processo e outro

estes deverão ser executados de forma seqüencial ou ainda se a pessoa ou equipe responsável por um processo for a mesma pelo outro também. O que eu quero dizer é que, dependendo da forma com que o processo foi implementado na organização, suas dependências ou ainda o tamanho da equipe responsável por ele, sua execução será ligeiramente alterada, mas isso não afetará suas atividades ou produto final. Acompanhe a seguir os 3 processos e suas atividades para a SMF GRC.

1. Estabelecendo a Governança de TI.

   Governança é um processo que começa de cima para baixo (Top-Down) e requer a participação de todos colaboradores em uma organização. São processos, conjunto de normas, responsabilidades, liderança, e tomada de decisão que determinam como a organização deve trabalhar com transparência. As principais atividades deste processo são:

   - Definir uma visão
   - Alinhar TI com o Negócio
   - Identificar regulamentos e padrões
   - Criar políticas

2. Avaliar, Monitorar e Controlar Riscos.

   O gerenciamento de riscos é uma atividade que visa mitigar os riscos presentes, futuros e recorrentes em uma organização e os serviços prestados por TI. Em longo prazo gerenciar riscos se torna um ótimo controle interno endereçando cada situação para resoluções mais rápidas e objetivas. As principais atividades deste processo são:

   - Endereçar os objetivos de gerenciamento
   - Identificar riscos
   - Analisar e priorizar riscos
   - Identificar controles
   - Analisar controles
   - Planejar e agendar implementações
   - Criar registros e Implementar controles
   - Operar controles
   - Aprender com esforços anteriores e atualizar a base de conhecimento

3. Obedecer as Políticas.

   Estar em conformidade é que as atividades aqui oferecem para a organização. As regulamentações, leis e políticas são cada vez mais abrangentes e exigem da organização certo nível de aderência, entre as principais leis presentes no dia-a-dia das organizações hoje são: Sarbanes-Oxley (SOX), a Health Insurance Portability and Accountability (HIPAA) e a Basiléia II. As principais atividades deste processo são:

   - Identificar políticas, leis, regulamentações e contratos
   - Selecionar políticas, leis, regulamentações e contratos
   - Avaliar o atual estado de conformidade
   - Definir um estado de conformidade futuro
   - Criar um plano de conformidade
   - Manter a conformidade
   - Auditar a conformidade

Conclusão

E assim terminamos mais um artigo sobre MOF 4.0, desta vez conhecemos os processos da SMF Governance, Risk and Compliance (GRC), no próximo artigo nós aprenderemos um pouco sobre as atividades da SMF Change and Configuration, até lá e muito obrigado pela leitura.

Bibliografia

Referências utilizadas na elaboração deste artigo:

1. Microsoft. www.microsoft.com
2. Microsoft Brasil. www.microsoft.com.br
3. Documentação oficial do MOF. www.microsoft.com/mof

Escreveu,

Cleber Marques
contato@clebermarques.com

Domingo, 27 de Abril de 2008.