Desenvolvido em 2009 pela Isaca o modelo é um complemento do CobiT dedicado a auxiliar no gerenciamento de riscos relacionados a TI.

Um risco pode ser classificado como uma oportunidade e/ou uma ameaça

Uma empresa corre o risco de ganhar muito dinheiro com o novo produto/serviço (oportunidade) ou corre o risco de ter um grande prejuízo (ameaça).

------------------------------------------------------------------------------------------------------------------------------

Grande parte dos riscos fogem do controle das empresas, portanto, a única opção é ter planos para caso os riscos se tornem verdade.

Sistema de Gerenciamento de Riscos da Organização ERM fornece uma estrutura que normalmente envolve a identificação de determinados riscos e oportunidades, avaliando-os em termos de probabilidade e magnitude do impacto, determinando uma estratégia de resposta, e monitorar o progresso.

------------------------------------------------------------------------------------------------------------------------------

A efetiva governança dos riscos de Ti

Conectada aos objetivos: o foco está no resultado do negócio, a ti apoia o atingimento dos objetivos do negócio

A quantidade de riscos com que a empresa está disposta a lidar é claramente definida.

E o processo de tomada de decisão da organização considera o conjunto completo de consequências e oportunidades em função dos riscos de TI.

Os riscos são priorizados de acordo com a tolerância aos riscos.

A gestão efetiva dos riscos de TI

Informação transparente sobre os riscos de TI é compartilhada e serve como base para a tomada de decisão relacionada aos riscos de TI.

As responsabilidades sobre a propriedade do risco estão claramente definidas e aceitas e decisões sobre riscos são tomadas por pessoas autorizadas com o foco na gestão do negócio

As práticas de gerenciamento de riscos são priorizadas e embutidas nos processos de tomada de decisão. ê As práticas de gerenciamento de riscos são diretas e fáceis de usar e contêm elementos para detectar ameaças e riscos potenciais, preveni-los e mitigá-los.

------------------------------------------------------------------------------------------------------------------

* Riscos para a agregação de benefícios/valor pela TI: associados com a perda de oportunidades de uso da TI para melhorar a eficiência e eficácia dos processos de negócio ou para promover novas iniciativas de negócio.
* Riscos para a entrega de projetos e programas de TI: associados com a contribuição da TI para melhorar o negócio ou para o desenvolvimento de novas soluções, na forma de programas e projetos.
* Riscos para a entrega de operações e serviços de TI: associados com todos os aspectos de desempenho dos sistemas e serviços de TI, que podem trazer a reduzir ou mesmo destruir o valor da empresa.

Teste