

ISO 31000

Risk Management e sua importância

Na visão holística, os controles dos processos e gestão de riscos de negócios nas empresas devem ser analisados pelo todo e não isoladamente. Ou seja, reunir os componentes dessa forma é reconhecer a importância da abordagem integrada. A continuidade da abordagem integrada permite vantagens estratégicas no competitivo cenário globalizado, que contribuem para a eficiência e melhoria nos processos e, conseqüentemente, dos resultados. Isso garante competitividade, sustentabilidade, governança, gestão de risco, redução de custos e erros para os negócios.

Por Wagner Fachetti



Para ser eficaz e garantir visão holística nos aspectos de controles dos processos de negócios da empresa, podemos utilizar uma abordagem GRC que integra os conceitos de Governança Corporativa, Gerenciamento de Riscos e Conformidade (GRC). A abordagem GRC – ou soluções de mercado como SAP BusinessObjects GRC Solution – pode ser aplicada a qualquer segmento de indústria e processo de negócio, independentemente do tamanho.

O tema GRC se tornou muito discutido e considerado destaque nos orçamentos de TI de algumas empresas com o surgimento, principalmente, da lei americana SOX (Sarbanes Oxley) criada em 2002. Regulamentos, a exemplo do SOX, que estabelecem regras de transparência para as empresas que negociam na bolsa de Nova Iorque, causaram impactos no dia-a-dia operacional das empresas. Isso ocorreu mediante a responsabilidade de estabelecer boas práticas e uma política eficaz de controle dos processos, objetivando a desejada transparência para os acionistas e o mercado.

Aparentemente, nem tudo que foi criado e realizado até agora nos aspectos de Governança Corporativa pareceu ser suficiente para evitar uma crise mundial, como a que enfrentamos hoje. Os sucessivos resultados negativos das empresas desde o início da crise financeira comprovam que leis (a exemplo da SOX, modelos de governança e gestão de riscos como COSO-ERM e AS/NZS 4360 - Risk Management) não foram suficientes para evitar o estabelecimento da crise financeira mundial. Inúmeros debates surgiram para discutir a eficácia e relacionamento da Lei SOX com a crise financeira.

Podemos considerar também como reflexo da crise financeira (e/ou na tentativa de se evitar uma) a criação de novas práticas, regras e políticas de governança corporativa impostas por comissões e organismos que ditam as regras no mercado. A PCAOB (Public Company Accounting Oversight Board), por exemplo, aumentou o foco nos controles dos riscos considerados mais críticos. Outro exemplo que se relaciona às políticas de gestão de riscos das empresas é o novo requerimento da Standard & Poor, que estabelece que as corporações serão avaliadas também pelas suas práticas de gestão de riscos.

Como não poderia ser diferente, a International Organization for Standardization – ISO* vem trabalhando para finalizar a norma internacional ISO 31000 que estabelece princípios e boas



FIGURA 1 – Componentes do framework Draft International Standard ISO/DIS 31000

práticas relacionadas ao tema Gestão de Riscos. O lançamento da versão final da norma internacional ISO 31000, no início do ano, teve no comitê de criação a participação brasileira.

Essa norma estabelece que a concepção do desenho e implementação da gestão do risco depende das necessidades da organização, objetivos específicos, contexto, estrutura, produtos, serviços, projetos, processos de exploração e práticas empregadas.

O framework para o gerenciamento de riscos (cláusula 5) propõe passos para desenvolver e manter um quadro de gestão de risco, bem como a forma como se inter-relacionam, conforme mostrado detalhadamente na figura 1, acima.

O desenho e implementação do quadro (figura 1) para a gestão de riscos deve levar em consideração o entendimento do contexto interno e externo da organização, que podem influenciar significativamente a sua concepção. São exemplos o contexto cultural, legal, financeiro, econômico, percepções, avaliações, conhecimento, etc. que é abordado na norma.

O padrão ISO 31000 adiciona também mais um guia de boas práticas para apoiar as empresas na adoção crescente de políticas de GRC nos seus processos de negócios. A nova norma não tem o objetivo de substituir outras já existentes, mas servir como complemento às atuais, além de regulamen-

tações específicas e locais de cada país.

O tema GRC veio para ficar e muitas empresas que o adotou já percebem as vantagens alcançadas, tanto nos aspectos de competitividade quanto os benefícios relacionados à redução de custos com o aperfeiçoamento e melhor controle dos processos.

O ponto de partida para essa reflexão sobre o tema GRC pode ser obtido pela análise do cenário, considerando: mapeamento dos requerimentos e objetivos do negócio da empresa; documentação dos processos de negócios, criação de políticas e procedimentos internos de âmbito corporativo para governança, conformidade e

gestão de risco, mapeamentos dos processos críticos e controles, etc.

O estabelecimento de uma política de governança pode ser acelerado através da utilização da solução SAP BusinessObjects para GRC. Essa solução é única no mercado com visão holística que possibilita integração e automação dos processos de governança.

Com o BusinessObjects para GRC, empresas podem aumentar o desempenho operacional e estratégico, reduzindo custo efetivo com cumprimento e conformidade com regulamentações e políticas, enquanto proativamente mitiga todos os tipos de riscos de negócios.

A figura 2 ilustra o framework SAP BusinessObjects para GRC, que avança a adoção de normas, Standards, frameworks e guide lines relacionados às melhores práticas de governança e gestão de risco reconhecidos atualmente pelo mercado. E a plataforma SAP NetWeaver também é parte importante nesse processo de estabelecimento de governança, além de possuir outras soluções para governança e conformidade: SAP Netweaver Identity Management, SAP Audit Management, SAP AIS, e SAP Solution Manager, etc..

WAGNER FACHETTI é coordenador do Grupo de Pesquisas e Estudos de Auditoria e GRC da ASUG Brasil.

Colaboraram: JOSÉ ANTONIO NUNES (Consultor Especializado SAP) e CLAUDIO ROCHA - FS LA GRC HUB Manager da SAP

SAP BusinessObjects GRC Solution



FIGURA 2 – SAP BusinessObjects GRC Solution

(*) Embora popularmente se acredite que a expressão "ISO" é uma sigla de "International Standards Organization", na realidade o nome originou-se da palavra grega "isos", que significa igualdade. Evita-se com isso que a organização possua diferentes acrônimos em diferentes idiomas, já que em inglês, o acrônimo seria IOS ("International Organization for Standardization"), em francês OIN ("Organisation Internationale de Normalisation"), e assim por diante. A escolha do nome "ISO" reflete assim o objetivo da organização, ou seja, a padronização entre as diversas culturas.