101 – Julho de 2008

IT GRC: o que significa na prática.

O termo GRC vem ganhando grande reconhecimento na área de negócio e representa uma nova abordagem integrada e adotada por organizações modernas para endereçar os temas Governança, Gerenciamento de Risco e Conformidade. São domínios com grande afinidade entre si e podem ser empregados em qualquer área da organização, apesar de estarem sendo mais largamente usados nas áreas financeira e de tecnologia da informação. Sua existência se deu como reflexo da percepção dos gestores de que era possível reduzir custos e aumentar a eficiência dos projetos que tratavam dos três temas de forma isolada através de um *framework* integrado. Tudo isso com o propósito legítimo de aumentar a eficiência dos negócios e adicionar valor através da melhoria dos processos de tomada de decisão e planejamento estratégico.

> Podemos descrever **Governança** como um atributo de administração dos negócios que procura criar um nível adequado de transparência através da definição clara de mecanismos de tomada de decisão e gestão que irão garantir a aderência aos processos e políticas estabelecidas.
>
> Gerenciamento ou **Gestão de Riscos**, por sua vez, pode ser entendido como o processo pelo qual uma empresa define seu apetite de risco, identifica os impactos potenciais e prioriza os limites de tolerância ao risco baseada nos objetivos de negócio.
>
> **Conformidade** ou simplesmente *Compliance,* em Inglês, é o processo que estabelece meios de registro e monitoramento de procedimentos, políticas e controles necessários para demonstrar aderência a requerimentos legais, políticas internas ou regulamentações setoriais.

Guardadas as devidas proporções e particularidades de cada negócio, a abordagem GRC propõe a redução de sobreposições e, portanto, de duplicação de esforço e custo para manter *frameworks* de governança como COSO (*Committee of Sponsoring Organizations of the Treatway Commission)*, ITIL (*Information Technology Infrastructure Library*) e COBIT (*Control Objectives for Information and related Technology*); *frameworks* de gestão de riscos como ISO270001 e *frameworks* de conformidade como SOX (Sarbanes Oxley), BASELII (Basiléia II) e ainda regulamentações setoriais específicas.

Como resultado da demanda crescente dos requerimentos de conformidade e o aumento do custo dos riscos, as empresas iniciaram a integração que passou proativamente a endereçar toda sorte de risco a partir de um único ponto de observação. O risco da informação, risco operacional e o próprio risco de não conformidade passaram a fazer parte do radar de GRC. Com isso, a área ganhou mais autonomia, poder, visibilidade, mas também responsabilidade, dado o impacto potencial que estes três domínios juntos podem gerar, positiva ou negativamente, no resultado (*bottom line)*, das empresas.

Para colocar tudo isso em prática, o primeiro passo deve ser mapear todos os requerimentos genéricos de governança, gestão de riscos e conformidade que incidem sobre todas as indústrias e então mapear aqueles específicos e inerentes à natureza da atividade comercial da empresa. A partir daí, é preciso reunir os *frameworks* implementados e mantidos pela empresa e procurar por sobreposições. Sejam atividades de gerenciamento de projetos, sejam atividades de desenvolvimento de políticas ou mesmo atividades regulares de teste de controle e *assurance*, é dado como certo encontrar pontos de redundância em que se pode empregar um esforço único, mais eficiente e econômico.
Se a empresa já emprega *frameworks* internacionais reconhecidos pelo mercado, é possível ainda ganhar tempo procurando por trabalhos que já oferecem o resultado do mapeamento entre diversos esquemas. A ISACA (*Information System Audit and Control Association*), por exemplo, disponibiliza análises completas que mapeiam os controles do COBIT contra diversos outros *frameworks* de segurança, conformidade e governança.

Com o primeiro passo completo, o próximo deve ser a adoção de uma abordagem baseada em risco, ou seja, assumindo o resultado da análise de riscos como a variável chave de definição de prioridades e, portanto, de classificação da importância dos controles multifuncionais que suportam um ou mais esquemas de *governance, risk e compliance*.
Nesta etapa já será possível ver os benefícios do GRC, pois ao invés de ter os originais três 'pratos' cheios de controles específicos, será possível ter agora um único prato com um número menor de controles, além de organizados e rotulados individualmente por sua relevância em relação a cada um dos esquemas de GRC, por exemplo, ISO27001 e SOX.

A experiência prática me diz que convém assumir um esquema de mais alto nível como o esquema mãe, como o COBIT, e então realizar os mapeamentos dos demais em relação a ele. Desta forma, tendo a tabela de mapeamento nas mãos, quando estivermos falando, por exemplo, de um controle de segurança ISO27001 relacionado à continuidade de negócios: *14.1.2 Business continuity and risk assessment*, visualizaremos sua relação direta como o objetivo de controle do COBIT: *DS4.1 IT continuity framework*, assim como sua relevância para o esquema de conformidade SOX ou qualquer outro relevante para a indústria em questão, baseado no rótulo do controle.

Sob o ponto de vista operacional, esta integração proporcionará uma linguagem comum entre os diversos níveis da organização bem como entre os diversos domínios e esquemas de governança, risco e conformidade, permitindo maior fluidez das decisões e o mais importante, a maximização dos investimentos a partir de uma visão integrada dos controles e suas implicações. Ao mesmo tempo, o longo e doloroso processo de definição e justificação dos orçamentos e investimentos será facilitado pela boa visibilidade que se terá da prioridade dos controles e seu papel nos diferentes esquemas.

É importante ainda reconhecer a necessidade de uma gestão eficiente da área de GRC, que mesmo integrando três grandes e complexos domínios, deverá manter mecanismos de acompanhamento de progresso segregado, onde se possa enxergar os principais *milestones* e requerimentos de *assurance* de cada esquema e reagir a eles adequadamente.

Garantia ou simplesmente *assurance*, em Inglês, é outro tema de extrema importância para o contexto de governança, risco e conformidade, pois é, na verdade, o resultado que se espera de um bom trabalho integrado feito pela área de GRC. Para isso, é crucial estabelecer um *framework* especial de *assurance* que irá definir os fluxos de relatório de progresso dos diferentes esquemas, os mecanismos para o armazenamento das evidências e ainda os diversos pontos de checagem de qualidade ao longo do trabalho. Tudo isso para evitar surpresas desagradáveis e a descoberta de que o trem estava fora dos trilhos quando já for tarde demais.

Ainda há muito mais sobre GRC e seus desafios para ser descoberto, desenvolvido e experimentado, mas é possível começar esta jornada acessando o site da OCEG (*Open Compliance and Ethics Group*) em www.oceg.org, associação sem fins lucrativos que, de maneira competente, promove a integração desses três importantes domínios.

Marcos Sêmola *é Global IT GRC Manager da Shell International Limited Gas & Power na Holanda, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor; Membro fundador do Institute of Information Security Professionals of London. MBA em Tecnologia Aplicada, Professor da FGV com especialização em Negociação e Estratégia pela London School, Bacharel em Ciências da Computação, autor de livros sobre gestão da segurança da informação, governança e inteligência competitiva. Visite www.semola.com.br ou contate marcos@semola.com.br*