O papel da TI no cumprimento de requisitos legais, normativos e de regulamentos setoriais (compliance)

Aderência do GFS/TQS aos requerimentos do Novo acordo de Capital da Basiléia (Basiléia II)

GFS Software e Consultoria Ltda
www.gfs.com.br

Introdução

Nos últimos anos assistimos a uma proliferação de leis, normas e regulamentos setoriais tais como Sarbanes-Oxley Act, Health Insuranec Portability and Accountability Act, Payment Card Industry Data Security Standard, Gramm-Leachy Bliley Act, SB 1386 e Basiléia II.

Cada uma delas possui contexto, implicações e objetivos específicos, mas em geral todas tem por princípio fundamental o estabelecimento de regras que garantam o cumprimento de boas práticas de governança corporativa e a transparência nas relações com o mercado.

É do senso comum que todas essas regulamentações possuem impacto direto, em maior e menor grau, sobre a maneira como as empresas processam e como armazenam a informação. Entretanto, paradoxalmente, é difícil encontrar uma organização que saiba definir claramente como o seu ambiente de sistemas deve ser adequado para atender às exigências das regulamentações que lhe afetam diretamente.

O principal motivo para essa dificuldade é que as regulamentações são de aplicação geral. Assim, estabelecem apenas os critérios mínimos sobre a forma de conduzir os negócios e não trazem recomendações específicas sobre como cuidar das informações. Por exemplo, os regulamentos falam em garantir a confidencialidade das informações mas não especificam como fazê-lo e nem quais ferramentas usar. Na realidade, caberá às próprias empresas, conhecedoras das especificidades de seus ambientes, pensarem nas soluções de TI necessárias para o cumprimento das exigências de negócio estipuladas.

Da mesma forma, como desenvolvedora de sistemas, o papel da GFS Software é mostrar aos clientes de que forma os aplicativos que desenvolve podem ajudá-los a adequar os seus ambientes às exigências das diversas regulamentações.

Em especial, o GFS/TQS – Tape Quality System é um aplicativo que foi concebido e especialmente projetado para ajudar às empresas a cumprir requerimentos de *compliance*. O objetivo desta série de documentos é mostrar como o TQS endereça as exigências de cada lei, norma ou regulamento.

O presente documento endereça especificamente as exigências do Novo Acordo de Capital da Basiléia (Basiléia II).

O Novo Acordo de Capital da Basiléia (Basiléia II)

Os acordos da Basiléia referem-se aos acordos de supervisão bancária (recomendações para a criação de projetos de lei), Basiléia I e Basiléia II, estabelecidos pelo Comitê de Supervisão Bancária da Basiléia (Basiléia é o nome da cidade suíça onde o comitê se reúne).

O comitê da Basiléia

É composto por representantes dos bancos centrais, autoridades supervisoras e organismos reguladores do setor financeiro dos países do G10 e de Luxemburgo e Espanha. O comitê não tem autoridade para exigir o cumprimento das recomendações, embora a maior parte dos países membros e até outros países não-membros tendam a implementar as políticas do comitê. Isso significa que as recomendações transformam-se em exigências através da criação de leis nacionais em cada país.

O acordo da Basiléia

Em linhas gerais o acordo da Basiléia preocupa-se com a gestão de riscos nas instituições bancárias. O princípio é estabelecer regras que minimizem os riscos e que protejam os bancos contra quebras na ocorrência destes, garantindo que os bancos retenham capital suficiente para cobrir perdas inesperadas.

Os riscos no setor bancário são os seguintes:

- Risco de crédito
- Risco país e risco de transferência
- Risco de mercado
- Risco de taxa de juros
- Risco de liquidez
- Risco operacional
- Risco legal
- Risco de reputação

Riscos minimizáveis através de esforços de TI

Os tipos de risco que podem ser gerenciados ou minimizados com o apoio de recursos de TI são os riscos operacional, legal e de reputação.

Risco operacional

As modalidades mais relevantes de risco operacional envolvem o colapso de controles internos e do domínio corporativo. Tais colapsos podem acarretar perdas financeiras por meio de erros, fraudes ou deficiências no desempenho oportuno de atividades, podendo ainda causar, de alguma outra forma, comprometimento dos interesses do banco, por exemplo, por seus representantes (*dealers*), agentes de concessão de crédito ou outros componentes administrativos, mediante excessos no uso de suas competências e atribuições, ou pela condução dos negócios de maneira não ética ou arriscada. Outras formas de risco operacional incluem deficiências graves nos sistemas tecnológicos de informação ou eventos como grandes incêndios ou outros desastres.

Risco legal

Os bancos estão sujeitos a várias formas de risco legal. Aí encontra-se incluído o risco de desvalorização de ativos ou de valorização de passivos em intensidades inesperadamente altas por conta de pareceres ou documentos legais inadequados ou incorretos. Adicionalmente, a legislação existente pode falhar na solução de questões legais envolvendo um banco. Um processo judicial envolvendo um determinado banco pode ter amplas implicações para todo o segmento bancário e acarretar custos, não somente para a organização diretamente envolvida, mas também para muitos ou todos os outros bancos. Ademais, pode haver mudanças nas leis que afetam bancos ou outras empresas comerciais. Os bancos são particularmente suscetíveis a riscos legais quando adotam novos tipos de transações e quando o direito legal de uma contraparte numa transação não está estabelecido. Ainda, num processo judicial podem ser impostas pesadas penalidades no caso do descumprimento de prazos para apresentação de documentos e informações.

Risco de reputação

Os riscos de reputação se originam, entre outras causas, de falhas operacionais e de deficiências no cumprimento de leis e de regulamentos relevantes. Riscos de reputação são particularmente danosos para bancos, já que a natureza de seus negócios requer a manutenção da confiança de depositantes, de credores e do mercado em geral.

Aderência de recursos de TI às exigências da Basiléia II

Os recursos de TI são aderentes às exigências do Novo Acordo de Capital da Basiléia sempre que colaboram para a redução do risco ou com as tarefas de controle e supervisão necessárias para o seu gerenciamento adequado.

Especificamente, uma aplicação ajuda a cumprir os requisitos da Basiléia II se implementa um ou mais dos seguintes processos / sistemáticas:

1. Prevenção à divulgação indevida das informações
2. Prevenção da realização de transações não autorizadas
3. Prevenção da realização de mudanças não autorizadas, realizadas em sistemas durante seu desenvolvimento ou manutenção, que possam permitir a realização de transações fraudulentas, retirar o controle e monitoração de determinadas operações ou desabilitar *logs* de auditoria (de modo a permitir que certas ações passem despercebidas).
4. Prevenção da interceptação e modificação de transações durante o processo de transmissão das informações através de canais de comunicação.
5. Prevenção da interrupção de serviços devido a falhas de hardware ou software.

A implementação destas características é obtida através de recursos de TI que procurem garantir os seguintes aspectos durante o processamento, transmissão e armazenamento das informações:

- Confidencialidade
- Integridade
- Disponibilidade
- Logs e trilhas de auditoria
- Autenticação / autenticidade

Como o GFS/TQS reduz riscos

O GFS/TQS foi especialmente desenhado para ajudar as empresas a atender requerimentos de *compliance* no armazenamento de informações em fitas magnéticas, minimizando ou eliminando alguns tipos de risco.

O GFS/TQS reduz riscos implementando recursos e funções para:

1. Prevenção da interrupção de serviços devido a falhas de hardware ou software – reduzindo a probabilidade de falhas em mídias e assegurando maior disponibilidade de informações críticas para a operação ou para o cumprimento de exigências legais
2. Prevenção da realização de transações não autorizadas – através da certificação de autenticidade, evidenciando a ocorrência de fraudes nos arquivos e tornando sua prática muito mais difícil.

Através de suas funções e características o GFS/TQS afetam positivamente os seguintes aspectos durante o processamento, transmissão e armazenamento das informações:

- Proteção da **integridade** dos arquivos
- Maior **disponibilidade** da informação
- Garantia de **autenticidade** do conteúdo de arquivos (prova de não-adulteração)

Redução do risco operacional

O emprego do GFS/TQS e a observação das condições por ele sinalizadas garante que fitas velhas e sem condições de uso sejam imediatamente identificadas e substituídas. Nestas condições, todas as demais fitas em uso numa organização estarão em condições de armazenar informações com confiabilidade.

Garantindo a presença apenas de fitas de boa qualidade e através de operações de certificação de leitura (que demonstram periodicamente a disponibilidade de informações críticas), o GFS/TQS minimiza a possibilidade da perda de dados vitais aos processos operacionais devido a falhas em mídias magnéticas.

Assim o GFS/TQS garante não somente a integridade como a disponibilidade das informações, reduzindo perdas por paradas em produção ou pela necessidade de reprocessamento.

Ao mesmo tempo, o GFS/TQS implementa importante recurso de controle de erros e fraudes: a certificação de autenticidade consegue demonstrar que os arquivos guardados não sofreram nenhum tipo de alteração, acidental ou intencional, reduzindo o risco de fraudes.

Redução do risco legal

Atualmente, boa parte das informações precisam ser mantidas íntegras e disponíveis durante períodos que excedem muito a durabilidade especificada, até mesmo das mídias mais modernas. Não são raros os casos onde é preciso guardar informações por 4 ou 5 décadas, quando as fitas mais modernas tem durabilidade em torno de 15 ou 20 anos.

A não disponibilidade da informação pode sujeitar a empresa a multas e outras penalidades, que podem incluir até mesmo a prisão dos representantes legais (por exemplo no caso do descumprimento de mandados judiciais exigindo a apresentação de informações dentro de prazos determinados).

O GFS/TQS identifica automaticamente as mídias que atingiram sua vida útil e movimenta os dados nelas contidas para mídias novas, assegurando a disponibilidade das informações que precisam ser arquivadas por longos períodos devido a exigências legais.

Ao mesmo tempo, a exclusiva funcionalidade de certificação de autenticidade do GFS/TQS é capaz de provar para autoridades e auditores a autenticidade dos arquivos exigidos.

O GFS/TQS mantém ainda uma base de dados completa sobre os arquivos guardados em fita. O produto inclui um amplo leque de relatórios capazes de demonstrar os esforços de controle de riscos sendo realizados, atendendo importantes requisitos de auditoria.

Redução do risco de reputação

Ao reduzir os riscos de ocorrências de falhas operacionais e de deficiências no cumprimento de leis e de regulamentos relevantes, o GFS/TQS acaba reduzindo também os riscos ligados à danos na reputação.

Referências

COMITÊ DE SUPERVISÃO BANCÁRIA DA BASILÉIA. **Princípios Essenciais para uma Supervisão Bancária Eficaz**. Tradução de Jorge R. Carvalheira. Brasília: Banco Central do Brasil , 1997. Disponível em: <http://www.bcb.gov.br/ftp/defis/basileia.pdf>. Acesso em: 21 dez. 2006.

SECURITY INNOVATION, INC. **Regulatory Compliance Demystified: An Introduction to Compliance for Developers**. [S.l]: Microsoft, 2006. Disponível em: <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/regcompliance_demystified.asp>. Acesso em: 21 dez. 2006.