

RFI – REQUEST FOR INFORMATION

ESCLARECIMENTOS III

ITEM 2.33:

A solução disponibiliza mecanismos para automatização e customização da solução via API ou outro recurso técnico? Comente a solução implementada, inclusive citando restrições quanto às possibilidades de customização pelo próprio Banco do Nordeste.

PERGUNTA 1:

Considerando que os termos “automatização” e “customização” são abrangentes e podem dar margem a várias interpretações, gentileza esclarecer e exemplificar o que se deseja com automatização e customização, para que possamos elaborar nossa resposta.

RESPOSTA:

A motivação deste requisito é saber se as funcionalidades da aplicação estão disponíveis para acesso mediante uma API (DLL, webservice ou outro formato qualquer).

ITEM 3.1:

O sistema terá que permitir o cadastramento das unidades administrativas e processos organizacionais, atentando para a possibilidade de níveis e subníveis tantos quantos forem os definidos pelo Banco, bem como o registro das datas de início e fim de vigência.

PERGUNTA 2:

Está sendo solicitado o registro das datas de início e de fim simplesmente para registro dessas datas ou espera-se que o sistema mantenha um controle de versões temporal dos dados do cadastro?

RESPOSTA:

No cadastro das unidades administrativas não precisa haver um controle de versão temporal, o registro das datas de início e fim é suficiente. Já no cadastro de processos organizacionais, o sistema precisa manter um controle de versão temporal das arquiteturas de processos do Banco.

ITEM 3.2:

O sistema terá que permitir o cadastramento automático das unidades administrativas e processos organizacionais, através da interligação com os sistemas do Banco, atentando para a possibilidade de níveis e subníveis tantos quantos forem os definidos pelo Banco, bem como o registro das datas

de início e fim de vigência.

PERGUNTA 3:

- a) **Como será feita essa “interligação com os sistemas do Banco”? Síncrona ou assíncrona? Quais os mecanismos de integração serão disponibilizados pelo Banco? Qual a plataforma dos sistemas a serem interligados?**
- b) **Está sendo solicitado o registro das datas de início e de fim simplesmente para o registro dessas datas ou espera-se que o sistema mantenha um controle de versões temporal dos dados do cadastro?**

RESPOSTA:

- a) No caso do cadastro de unidades administrativas a integração pode ser do tipo assíncrona, por meio de uma importação periódica de dados do sistema do Banco.
- b) No cadastro das unidades administrativas não precisa haver um controle de versão temporal, o registro das datas de início e fim é suficiente. Já no cadastro de processos organizacionais, o sistema precisa manter um controle de versão temporal das arquiteturas de processos do Banco, possibilitando definir equivalências entre processos.
- c) A empresa deve explicar como pretende implementar as integrações, considerando que os sistemas legados do Banco podem ser na arquitetura Cliente_Servidor, que rodam na plataforma Windows, com Sql Server ou WEB 3 camadas, utilizando componentes COM+ e WebServices, aplicativos Java executando no Mainframe, com DB2, e sistemas de processamento Batch executando no Mainframe.

ITEM 3.4:

O sistema terá que permitir o cadastramento dos usuários, por nível de acesso e unidades administrativas e ou processos auditáveis, de acordo com o perfil definido pelo Banco, atentando para o registro da data de início e fim de vigência.

PERGUNTA 4:

Está sendo solicitado o registro das datas de início e de fim simplesmente para registro dessas datas ou espera-se que o sistema mantenha um controle de versões temporal dos dados do cadastro?

RESPOSTA:

O cadastro de usuários do sistema deve ser integrado, de forma on-line, com o cadastro de pessoal do Banco. Na concessão de permissões de acesso ao sistema devem ser considerados alguns dados funcionais atuais, tais como: função que o usuário ocupa e sua unidade de lotação atual. Espera-se um controle de versões temporal das permissões e grupos de acesso.

ITEM 3.5:

O sistema terá que permitir o cadastramento automático dos usuários, por nível de acesso e unidades administrativas e ou processos auditáveis, através da interligação com o sistema de segurança, conforme o perfil definido pelo Banco, atentando para o registro das datas de início e fim de vigência.

PERGUNTA 5:

- a) Em que consiste o “cadastro automático de usuários”?
- b) Esse “cadastro automático de usuários” será feito mediante importação periódica dos dados do sistema de segurança do Banco? Será síncrona ou assíncrona?
- c) Como será feita essa interligação com o sistema de segurança? Síncrona ou assíncrona? Quais mecanismos de integração serão disponibilizados pelo Banco? Qual a plataforma dos sistemas a serem interligados?
- d) Está sendo solicitado o registro das datas de início e de fim simplesmente para registro dessas datas ou espera-se que o sistema mantenha um controle de versões temporal dos dados do cadastro?

RESPOSTA:

O cadastro de usuários do sistema deve ser integrado de forma on-line com o cadastro de pessoal do Banco e espera-se um controle de versões temporal das permissões e grupos de acesso ao sistema.

ITEM 3.6:

O sistema terá que permitir o cadastramento de grupo de usuários, por nível de acesso e unidades administrativas e ou processos auditáveis, de acordo com o perfil definido pelo Banco, atentando para o registro das datas de início e fim de vigência.

PERGUNTA 6:

Está sendo solicitado o registro das datas de início e de fim simplesmente para registro dessas datas ou espera-se que o sistema mantenha um controle de versões temporal dos dados do cadastro?.

RESPOSTA:

Espera-se um controle de versões temporal das permissões e grupos de acesso ao sistema.

ITEM 3.7:

O sistema terá que permitir o cadastramento automático de grupo de usuários, por nível de acesso e unidades administrativas e ou processos auditáveis, através da interligação com o sistema de

segurança, conforme o perfil definido pelo Banco, atentando para o registro das datas de início e fim de vigência.

PERGUNTA 7:

- a) Em que consiste o “cadastro automático de grupo de usuários”?
- b) Esse “cadastro automático de grupo de usuários” será feito mediante importação periódica dos dados do sistema de segurança do Banco? Será síncrona ou assíncrona?
- c) Como será feita essa interligação com o sistema de segurança? Síncrona ou assíncrona? Quais mecanismos de integração serão disponibilizados pelo Banco? Qual a plataforma dos sistemas a serem interligados?
- d) Está sendo solicitado o registro das datas de início e de fim simplesmente para registro dessas datas ou espera-se que o sistema mantenha um controle de versões temporal dos dados do cadastro?

RESPOSTA:

Significa que apenas determinados usuários da rede corporativa deverão ter acesso ao sistema, a depender de sua função e lotação no momento do acesso. O cadastro de usuários do sistema deve ser integrado de forma síncrona com o cadastro de pessoal do Banco que contém as informações da função e lotação atual dos funcionários. O sistema de pessoal roda em plataforma Windows com SGBD SQL Server.

Espera-se um controle de versões temporal das permissões e grupos de acesso ao sistema.

ITEM 3.8:

O sistema terá que permitir o cadastramento de usuários e ou grupo de usuários por tipo de perfil, envolvendo no mínimo as seguintes atividades – incluir, alterar, consultar, excluir, aprovar, solicitar aprovação, comunicar, administrar, habilitar, desabilitar, gravar, criar, contendo para cada um deles e para outros a serem criados, se necessário, as datas de início e fim da vigência, para cada permissão, dentre outras, vinculando-os a unidades administrativas e ou processos auditáveis e ou papéis de trabalho de auditoria e ou documentos.

PERGUNTA 8:

- a) Entendemos que as transações de acesso explicitadas nesse item 3.8 da RFI são apenas exemplos, visto que para cada transação e operação do sistema existem transações específicas, e o que se quer é que o sistema tenha o controle das transações mais importantes do sistema. Nosso entendimento está correto?
- b) Está sendo solicitado o registro das datas de início e de fim simplesmente para registro dessas datas ou espera-se que o sistema mantenha um controle temporal dos dados do cadastro?

RESPOSTA:

Sim, as transações de acesso explicitadas são exemplos de possíveis atividades realizadas pelos usuários. Espera-se que o sistema possua um controle de versões temporal das permissões e grupos de acesso ao sistema.

ITEM 3.9:

O sistema terá que permitir a vinculação entre usuários e ou grupos de usuários em relação às unidades administrativas e ou processos auditáveis sob sua responsabilidade, com o estabelecimento do perfil mínimo de acesso para execução das atividades, bem como o registro das datas de início e fim de vigência.

PERGUNTA 9:

Está sendo solicitado o registro das datas de início e de fim simplesmente para registro dessas datas ou espera-se que o sistema mantenha um controle temporal dos dados do cadastro?

RESPOSTA:

Espera-se que o sistema possua um controle de versões temporal das permissões e grupos de acesso ao sistema.

ITEM 3.10:

O sistema terá que permitir efetuar alterações nas combinações entre unidades administrativas, processos auditáveis, usuários e grupo de usuários, de acordo com o interesse do Banco, sem atender as vinculações originais, atentando para o registro das datas de início e fim de vigência.

PERGUNTA 10:

Está sendo solicitado o registro das datas de início e de fim simplesmente para registro dessas datas ou espera-se que o sistema mantenha um controle temporal dos dados do cadastro?

RESPOSTA:

Espera-se que o sistema possua um controle de versões temporal das permissões e grupos de acesso ao sistema.

ITEM 3.11:

O sistema terá que permitir o cadastramento de usuários e órgãos externos ao Banco, com registro de datas de início e fim da vigência de permissão, que poderão consultar informações e encaminhar

documentos a serem inseridos no sistema.

PERGUNTA 11:

Está sendo solicitado o registro das datas de início e de fim simplesmente para registro dessas datas ou espera-se que o sistema mantenha um controle temporal dos dados do cadastro?

RESPOSTA:

Espera-se que o sistema possua um controle de versões temporal das permissões e grupos de acesso ao sistema.

ITEM 3.12:

O sistema terá que permitir a migração de unidades administrativas e ou processos auditáveis para outras unidades administrativas e ou processos auditáveis, por conta da extinção, aglutinação ou criação de novas unidades administrativas e ou processos auditáveis, atentando para a existência de níveis e subníveis existentes, destacando-se a necessidade de registros de datas de início e fim de vigência.

PERGUNTA 12:

Está sendo solicitado o registro das datas de início e de fim simplesmente para registro dessas datas ou espera-se que o sistema mantenha um controle de versões temporal dos dados do cadastro?

RESPOSTA:

Os objetos de auditoria possuem um órgão gestor e estão relacionados à arquitetura de processos organizacionais do Banco. O sistema deve prever a possibilidade de haver mudanças na estrutura organizacional da instituição. Espera-se que o sistema possua um controle de versões temporal dessas mudanças.

ITEM 3.14:

O sistema terá que manter registro de posições históricas no caso de migração de unidades administrativas e de processos auditáveis para outras unidades administrativas e processos.

PERGUNTA 13:

Entendemos que se o sistema possibilitar a migração de unidades administrativas e de processos auditáveis e o armazenamento do histórico dessas migrações em LOG, esse item estaria atendido. Está correto nosso entendimento?

RESPOSTA:

Espera-se que o sistema possua um controle de versões temporal das solicitações de baixa e repactuação de prazos das recomendações de auditoria, informando a unidade e o processo de origem da época em que foram feitos os registros no sistema.

ITEM 3.15:

O sistema terá que permitir a exclusão de unidades administrativas e processos auditáveis, por parte do administrador do sistema, desde que todos os documentos vinculados a esta estrutura já não existam ou estejam transferidas para outras vinculações.

PERGUNTA 14:

- a) O que devemos entender como “documentos vinculados”? Seriam recomendações, constatações, planos de ação, trabalhos de auditoria e relatórios de auditoria? Se sim, em qual situação deverão ser considerados pendentes? qual
- b) A transferência de “documentos vinculados” para outras unidades, dependendo da definição e da abrangência do termo, não causaria inconsistência no sistema, visto que se perderia o contexto de sua criação?
- c) Dependendo da granularidade e da resposta do item “a)” anterior, não seria o caso de se fazer o registro da migração em cada item de informação, ou seja, em cada recomendação, constatação e planos de ação?

RESPOSTA:

Deverão ser considerados pendentes os documentos (registro de constatação, Relatório de Auditoria etc.) ou eventos (repactuação de prazo solicitação de baixa de recomendação etc.) que ainda não foram encerrados e que poderão ainda tramitar. Entenda-se unidades administrativas e processos auditáveis como objetos de auditoria. Um objeto de auditoria poderá ter um ou mais órgãos intervenientes (gestores e executores de processos) e estarem associados a um ou mais processos da estrutura organizacional do Banco.

Caso um órgão interveniente ou processo organizacional associado ao objeto de auditoria deixe de existir, por exemplo, todas as pendências a ele relacionadas devem ser migradas para o novo interveniente e ou o novo processo.

O sistema não deverá permitir a exclusão de um objeto de auditoria caso ele esteja sendo referenciado em outras tabelas do banco de dados.

ITEM 3.18:

O sistema terá que permitir decompor os subprocessos e processos em atividades, tarefas e passos.

PERGUNTA 15:

A composição das atividades em tarefas e passos, imaginando a quantidade de macroprocessos e processos do BNB, não geraria uma quantidade de informações muito grande a ponto de inviabilizar o levantamento, registro no sistema, priorização e controle dos processos do Banco? Com base em implantações realizadas em outros clientes, entendemos que até o nível atividade seria suficiente. Está correto nosso entendimento?

RESPOSTA:

Apenas as atividades de maior complexidade seriam detalhadas no nível de tarefas e passos. O sistema de gestão de riscos utilizado no Banco também adota o conceito de tarefas e passos e precisamos estar compatíveis com ele.

ITEM 3.23:

O sistema terá que manter um catálogo com os domínios das atividades, possíveis locais onde uma atividade é executada (exemplo: superintendência estadual, agência, central de retaguarda).

PERGUNTA 16:

Entendemos que a informação de gestor do processo e tipo de unidade organizacional (diretoria, superintendência, agência) seria suficiente para se identificar o “domínio”. Está correto nosso entendimento?

RESPOSTA:

O domínio refere-se ao tipo de órgão onde a atividade é executada e não ao gestor do processo. Um processo pode ter várias atividades realizadas em agência, outras em uma central de retaguarda operacional, outras na Direção Geral do Banco, etc. Precisamos associar a atividade ao domínio. Uma atividade pode ser realizada em um ou mais domínios.

ITEM 3.24:

O sistema terá que permitir caracterizar uma atividade com sua respectiva descrição, domínio, objetivos, riscos e controles.

PERGUNTA 17:

Entendemos que a informação de gestor do processo e tipo de unidade organizacional (diretoria, superintendência, agência) seria suficiente para se identificar o “domínio”. Está correto nosso entendimento?

RESPOSTA:

O domínio refere-se ao tipo de órgão onde a atividade é executada e não ao gestor do processo. Um processo pode ter várias atividades realizadas em agência, outras em uma central de retaguarda operacional, outras na Direção Geral do Banco, etc. Precisamos associar a atividade ao domínio. Uma atividade pode ser realizada em um ou mais domínios.

ITEM 3.26:

O sistema terá que permitir classificar o controle quanto ao tipo, a partir de um catálogo de tipos de controles.

PERGUNTA 18:

O que devemos entender como “tipo de controle”? Gentileza exemplificar.

RESPOSTA:

São exemplos de tipo de controle: Alçadas e Limites, Autorizações, Conciliação, Acesso Físico etc. Um controle pode estar associado a um ou mais tipos.

ITEM 3.27:

O sistema terá que permitir indicar se o controle já é verificado ou não pela Área de Controles Internos da Instituição.

PERGUNTA 19:

- a) **As áreas de controles internos e de gestão de riscos serão usuárias da solução?**
- b) **A indicação solicitada seria feita pelo auditor ou pelas áreas de Controles Internos e de Gestão de Riscos?**
- c) **Em qual momento (ex: planejamento anual, planejamento do trabalho, execução) seria feita a indicação solicitada?**
- d) **Não seria o caso de se ter um catálogo corporativo de processos do Banco com informações compartilhadas sobre controle para que áreas de governança (Auditoria Interna, Controles Internos e Gestão de Riscos) possam utilizá-lo e mantê-lo corporativamente?**

RESPOSTA:

O indicador é um atributo do tipo bit (sim ou não). A indicação é feita pelo auditor durante o mapeamento do processo, quando do cadastramento dos objetivos, riscos e controles no sistema. Para cada controle cadastrado deve ser indicado se ele já é ou não verificado pela Área de Controles Internos.

ITEM 3.29:

O sistema deverá emitir o programa de auditoria, por macroprocesso ou processo auditável, com, no mínimo, as seguintes informações: a) relação dos objetos de auditoria subordinados com as respectivas definições e objetivos; b) representação gráfica da estrutura hierárquica dos objetos de auditoria subordinados; c) fronteiras com outros macroprocessos e processos organizacionais; d) quantitativo de processos, subprocessos e atividades, com os respectivos percentuais de atividades críticas; e) quantitativo de recomendações de auditorias referentes aos processos e subprocessos subordinados, com os respectivos percentuais de recomendações pendentes de regularização; f) possíveis escopos, focos e visões para os trabalhos de auditoria; g) técnicas e procedimentos de auditoria; h) orientações complementares necessárias à realização dos trabalhos de auditoria; i) ciclo de auditoria e datas previstas para realização dos trabalhos.

PERGUNTA 20:

- a) O BNB possui um sistema corporativo de mapeamento de processos?
- b) Considerando a descrição e a especificidade das informações desse Item, relacionadas com BPM (Business Process Management), não seria mais viável realizar uma integração com o sistema de processos corporativos (BPM), como por exemplo, a solução de BPM IBM Websphere Process Server a fim de evitar duplicidade e de se ter uma aplicação apropriada BMServer, para gestão de processos?

RESPOSTA:

O programa de auditoria consiste de um documento que planeja o ciclo de auditoria em um processo com os procedimentos necessários à orientação para realização de auditorias (descrição do objeto de auditoria, escopo, métodos e técnicas, estimativas de recursos, abordagens, responsabilidade) e as datas previstas para realização dos trabalhos envolvidos. Algumas informações desse relatório devem ser extraídas do sistema.

ITEM 3.32:

O sistema terá que emitir relatório do mapeamento do processo auditável com as respectivas atividades, objetivos, riscos e controles.

PERGUNTA 21:

O BNB possui um sistema corporativo de mapeamento de processos? Se sim, esse item não seria melhor atendido por solução de BPM, como por exemplo, IBM Websphere Process Server ou BMServer?

RESPOSTA:

A auditoria tem seu próprio cadastro de mapeamento de processos, com as atividades, objetivos,

riscos e controles identificados durante o estudo do processo na pré-auditoria. A integração com uma solução BPM está prevista, porém, não eliminará a necessidade das informações levantadas pelos auditores nos trabalhos de auditoria.

ITEM 3.33:

O sistema terá que emitir relatório do programa de auditoria, por macroprocesso ou por objeto de auditoria, com opção de imprimir o programa de auditoria completo ou aplicando filtros pré-definidos pelo usuário.

PERGUNTA 22:

Entendemos que um relatório em tela, como por exemplo, uma consulta que possibilite a visualização dos programas de auditoria seria suficiente. Está correto nosso entendimento?

RESPOSTA:

O programa de auditoria também deve poder ser impresso em formato de relatório. A Auditoria poderá precisar de um relatório único que englobe os diversos programas de auditoria relativos aos processos que formam um determinado macroprocesso, por exemplo.

ITEM 3.40:

O sistema terá que garantir que a matriz de criticidade, depois de validada, apenas possa ser modificada se o responsável pela validação autorizar sua reabertura antes do encerramento do trabalho de auditoria naquele processo.

PERGUNTA 23:

Entendemos que o controle do acesso à matriz de priorização, de forma que apenas pessoas autorizadas possam: criar, alterar e publicar; seria suficiente. Está correto nosso entendimento?

RESPOSTA:

Os usuários autorizados a editar a matriz limitam-se apenas aos auditores envolvidos no trabalho de auditoria. Adicionalmente, a matriz apenas poderá ser alterada por eles caso o trabalho de auditoria ainda não tenha sido encerrado. Caso o trabalho já tenha sido encerrado, a matriz apenas poderá ser alterada pela equipe de auditores com a prévia autorização do gestor responsável.

ITEM 3.68:

O sistema terá que permitir caracterizar o quesito do programa de testes com sua descrição, texto para ajuda, objetivo, tipo de população, indicador de auditoria contínua (sim ou não), texto sugerido para a constatação; texto sugerido para a recomendação; tempo previsto para a aplicação do teste.

PERGUNTA 24:

Entendemos que o atendimento desse item seria inviável pelos seguintes motivos:

a) Uma constatação poderá ser elaborada com base na interpretação da aplicação de vários roteiros de auditoria, programas de auditoria, papéis de trabalho e testes, ou seja, não há uma relação definida entre programa de testes e constatação.

b) Uma recomendação poderá ser elaborada com base em uma ou mais constatações que por sua vez são elaboradas com base na interpretação da aplicação de vários roteiros de auditoria, programas de auditoria, papéis de trabalho e testes, ou seja, não há uma relação definida entre programa de testes, constatação e recomendações.

c) O tempo para aplicação do teste é variável em função de vários fatores, dentre os quais: conhecimento do auditor sobre o processo; experiência do auditor; disponibilidade de documentos; contexto operacional da auditoria, dentre outros.

d) A indicação automática de constatação e de recomendação para programas de auditoria não é prática recomendada pelos institutos de auditoria, dentre os quais, o THEIA, visto que a constatação é produto intelectual do auditor, conforme explicações “a)” e “b)” acima e uma sugestão poderia cercear a necessidade e a capacidade de análise e interpretação do auditor e restringir e direcionar a análise do auditor.

e) Os tipos de população e de amostra estariam registrados na amostra e não no programa de auditoria, visto que um programa de auditoria poderia ser aplicado a várias amostras ou populações.

Nosso entendimento está correto?

RESPOSTA:

O sistema terá que fornecer um catálogo de perguntas por objeto de auditoria e na construção de um novo programa de testes de auditoria o auditor poderá importar perguntas desses catálogos. Após importadas as perguntas, estas poderão ser personalizadas de acordo com cada trabalho. O tempo estimado de aplicação de cada teste é uma informação gerencial para estimativa da duração do trabalho. O tipo de população e tipo de amostra são atributos que informam sobre que elementos da amostra devem ser aplicadas (ex: clientes, operações etc.).

Com relação aos textos padrões para constatação e recomendação o entendimento está correto.

ITEM 3.73:

O sistema terá que indicar o percentual de aplicação do programa de testes (total de quesitos aplicados / total de quesitos do programa de testes).

PERGUNTA 25:

A informação solicitada com base na fórmula apresentada não forneceria uma informação subjetiva e distorcida na maioria dos casos, visto a diversidade de programas e testes em relação à: abrangência, análise, complexidade e procedimentos?

RESPOSTA:

A informação solicitada tem a finalidade de acompanhar, por auditor, o andamento dos trabalhos de execução de auditoria. O sistema terá que informar ao gestor sobre o andamento dos trabalhos e essa é uma das medidas possíveis.

ITEM 3.79:

O sistema terá que permitir definir o fluxo e papéis de trabalho por modalidade de auditoria (exemplo: fases previstas, regras para conclusão das fases do trabalho).

PERGUNTA 26:

O que seria “fluxo”. Gentileza exemplificar.

RESPOSTA:

O fluxo se refere à seqüência de fases previstas, por tipo de trabalho. Por exemplo: em um trabalho de auditoria do tipo especial, poderão existir apenas as fases de execução e comunicação de resultados. Já em uma auditoria do tipo Processos Corporativos, poderão existir as fases de Pré-auditoria, Execução e Comunicação de Resultados.

ITEM 3.94:

O sistema terá que permitir registrar os tipos de usuários que devem assinar cada tipo de papel de trabalho de auditoria.

PERGUNTA 27:

Entendemos que se o sistema possibilitar a definição de quem assina os relatórios de auditoria esse item estaria atendido.

Nosso entendimento está correto?

RESPOSTA:

O sistema terá que possibilitar definir quem assina cada tipo de papel de trabalho (Ex: Registro de Fragilidade do Processo, Carta de Encaminhamento, Relatório de Auditoria etc.). Os signatários de um tipo de relatório poderão ser diferentes dos signatários de outro tipo de documento.

ITEM 3.95:

O sistema terá que permitir definir o fluxo de validação para cada tipo de papel de trabalho de auditoria, com a definição dos responsáveis pela validação e a ordem de tramitação para validação.

PERGUNTA 28:

O que seria “fluxo de validação para cada tipo de papel de trabalho”. Gentileza exemplificar.

RESPOSTA:

O fluxo de validação consiste da definição da seqüência de responsáveis que devem validar cada tipo de papel de trabalho de auditoria. Por exemplo: Uma possível seqüência do fluxo de validação do relatório de auditoria poderia ser: 1º auditor coordenador, 2º gerente da célula de execução de auditoria e 3º gerente do ambiente de auditoria. Já para o documento Fragilidades do Processo o fluxo poderia envolver apenas o auditor coordenador e depois o gerente da célula de execução de auditoria.

ITEM 3.98:

O sistema terá que permitir definir *layouts* diferenciados para cada tipo de papel de trabalho de auditoria.

PERGUNTA 29:

O que deve ser customizável no layout O que se deseja seria um gerador de relatórios de mercado?

RESPOSTA:

O sistema terá que permitir a existência de diferentes modelos de papeis de trabalho, com layout definidos pelo Banco, tais como: Síntese de Auditoria, Relatório de Auditoria, Falhas de Execução do Processo, Fragilidades do Processo, Itens par Melhoria ou Medidas Corretivas, dentre outros. Por exemplo: caso a constatação identificada pelo auditor seja uma falha, a ocorrência será registrada no documento ‘Falha de Execução do Processo’ mas se for uma fragilidade será registrada no documento ‘Fragilidades do Processo’.

ITEM 3.102:

O sistema deverá garantir por meio de mecanismos criptográficos o sigilo das informações armazenadas, transmitidas e apresentadas.

PERGUNTA 30:

a) Entendemos que o que está sendo pedido é:

Que as informações sejam encriptadas e armazenadas no banco de dados dessa forma. Está correto nosso entendimento?

Se nosso entendimento estiver equivocado, gentileza esclarecer. Se nosso entendimento estiver correto, a adoção desse mecanismo traria os seguintes problemas:

i) A pesquisa textual e estruturada dos dados tornar-se-ia inviável.

ii) O tempo decorrido entre a solicitação da informação e exibição do resultado para o usuário, para os casos em que fossem viáveis, seria muito longo em função dos processamentos decorrentes da encriptação e desencriptação dos dados.

b) Que as informações trafeguem na rede por um canal encriptado. Se nosso entendimento estiver equivocado, gentileza esclarecer. Se nosso entendimento estiver correto, entendemos que a encriptação do meio de transmissão de dados cabe à infra-estrutura de rede do Banco, como por exemplo, uso do protocolo HTTPS, e não ao sistema. Está correto nosso entendimento?

c) Que as informações sejam apresentadas encriptadas e que seja pedida uma senha ou um certificado digital para desencriptar a informação para exibição para o usuário final. Está correto nosso entendimento? Se nosso entendimento estiver equivocado, gentileza esclarecer. Se nosso entendimento estiver correto, o tempo decorrido entre a solicitação da informação e exibição do resultado para o usuário, para os casos em que fossem viáveis, seria muito longo em função dos processamentos decorrentes da encriptação e desencriptação dos dados.

d) Quais os dados e documentos seriam passíveis dos processos de encriptação/desencriptação especificados?

Apenas para ilustrar o impacto da solicitação, informamos que nosso sistema possui cerca de 360 tabelas.

RESPOSTA:

Os argumentos apresentados pela empresa estão corretos. O fornecedor terá que explicar de que forma o sigilo das informações armazenadas, transmitidas e apresentadas será garantido.

ITEM 3.114:

O sistema terá que permitir definir e atualizar o layout do PAINT e as consultas necessárias à sua emissão de acordo com as necessidades da Área de Auditoria.

PERGUNTA 31:

O que deve ser customizável no layout? O que se deseja seria um gerador de relatórios de mercado?

RESPOSTA:

O sistema terá que permitir a emissão do Plano Anual de Auditoria Interna (PAINT) e a obtenção das informações necessárias ao seu preenchimento. A estrutura do relatório deve ser customizável para permitir possíveis alterações no modelo do documento. A empresa deve informar qual solução fornece para a emissão do PAINT.

ITEM 3.122:

O sistema terá que acompanhar, em tempo real, a realização dos trabalhos previstos no PAINT, indicando o percentual de realização.

PERGUNTA 32:

Quem informará o percentual de realização? O auditor ou o sistema calculará automaticamente? Se for o auditor, essa informação não seria precisa e passível de ficar desatualizada como já ocorreu em outras implantações em que, na maioria dos casos, os trabalhos saíam de 0% para 100% ao final da execução, ou seja, essa informação perdeu a credibilidade e deixou de ser utilizada. Por isso, acreditamos que a exibição dos trabalhos em andamento atenderia. Nosso entendimento está correto?. Se for calculado pelo sistema, como o BNB imaginaria o cálculo dessa informação?

RESPOSTA:

O sistema além de informar a situação atual dos trabalhos (ex: previsto, em andamento, concluído) terá que calcular o percentual de evolução da aplicação dos programas de testes de auditoria para permitir aos gestores estimar sua conclusão. Se um programa de testes tem 100 perguntas e está sendo aplicado em 10 unidades distintas, o sistema deve considerar no cálculo, por exemplo, quantas vezes a pergunta deve ser aplicada e quantas já foram respondidas. O cálculo poderá ser por unidade, por auditor, programa de teste ou de forma global.

ITEM 3.126:

O sistema terá que permitir definir e atualizar o layout do RAINT e as consultas necessárias à sua emissão de acordo com as necessidades da Área.

PERGUNTA 33:

O que deve ser customizável no layout? O que se deseja seria um gerador de relatórios de mercado?

RESPOSTA:

O sistema terá que permitir a emissão do Relatório Anual das Atividades de Auditoria (RAINT) e a obtenção das informações necessárias ao seu preenchimento. A estrutura do relatório deve ser customizável para permitir possíveis alterações no modelo do documento. A empresa deve informar qual solução fornece para a emissão do RAIN.T.

ITEM 3.136:

O sistema terá que emitir relatório do papel de trabalho 'Plano Operacional', por trabalho de auditoria ou objeto de auditoria.

PERGUNTA 34:

Entendemos que a geração do relatório de planejamento do trabalho de auditoria e a exibição dos papéis de trabalho em tela atenderiam a esse item. Está correto nosso entendimento?

RESPOSTA:

O Plano Operacional de Auditoria é um relatório que deve ser emitido pelo sistema. Esse documento tem como finalidade abordar o detalhamento do objeto, com ênfase no escopo do trabalho, procedimentos, recursos específicos, cronograma de atuação e resultados esperados. O Plano Operacional, resultante desse planejamento, representa as condições e os procedimentos necessários à realização de uma auditoria.

O preenchimento das informações iniciais do Plano Operacional é feito no início do trabalho podendo haver incremento de informações e ou modificações no decorrer do trabalho de auditoria. É necessário haver um controle de versões do Plano Operacional as quais devem ser aprovadas pelo auditor coordenador e pelo gerente da célula de execução de auditoria em determinadas etapas do trabalho.

ITEM 3.146:

O sistema terá que permitir registrar constatações referentes a um objeto de auditoria a qualquer tempo, independentemente de haver um trabalho de auditoria em andamento.

PERGUNTA 35:

Não entendemos como seria possível o registro de constatações, recomendações, relatórios de auditoria e a realização de um follow-up sem a realização de um trabalho de auditoria, visto que isso fere aspectos operacionais fundamentais de metodologia e requisitos de sistema apresentados em outros itens da RFI. Uma constatação não seria o objeto de análise do auditor e decorrente de testes? O BNB quer poder registrar constatações sem base em processos e programas de auditoria? Como ficariam as classificações e as

relações com outras informações do sistema requeridas nesta RFI, inclusive emissão de relatórios? Gentileza esclarecer.

RESPOSTA:

O sistema deverá permitir o registro de constatações avulsas, para possibilitar a geração de papeis de trabalho (ex: registro de constatação) referentes a objetos de auditoria que não possuem trabalho de auditoria em andamento. Por exemplo: um auditor poderá estar realizando uma auditoria no processo 'Concessão de Limite de Crédito para Cliente' e encontrar uma fragilidade de criticidade alta relacionada ao processo 'Cadastro de Clientes'. Nesse caso, o sistema terá que permitir o encaminhamento do problema para o responsável pelo processo 'Cadastro de Clientes' para que sejam dados os tratamentos necessários e a posterior emissão do documento 'Fragilidades do Processo' para o processo 'Cadastro de Clientes', se for o caso. Nesse caso específico, não havia nenhum trabalho de auditoria sendo realizado no processo Cadastro de Clientes e a constatação não surgiu da aplicação de um programa de testes de auditoria. Essa é apenas uma das situações que podem originar essa necessidade.

ITEM 3.152:

O sistema terá que permitir parametrizar, de forma histórica, as regras para repactuação de prazos de recomendações, considerando, entre outras características, o tipo (falha ou fragilidade), a abrangência, a criticidade, o prazo adicional, o destinatário e o responsável pela autorização de repactuação de prazo.

PERGUNTA 36:

Não entendemos o que seria "...parametrizar, de forma histórica...", as "...regras para repactuação de prazos...". Gentileza esclarecer e exemplificar.

RESPOSTA:

Significa definir as regras atuais sem excluir as antigas. Por exemplo: se em 01/01/2010 existir a regra "a repactuação de prazos das recomendações de criticidade alta e de abrangência corporativa devem ser autorizadas pelo superintendente estadual" e em 01/07/2010 a regra passar a ser "a repactuação de prazos das recomendações de criticidade alta e de abrangência corporativa devem ser autorizadas pelo presidente", o sistema terá que guardar esse histórico.

ITEM 3.165:

O sistema terá que gravar, em mídia removível, para uso fora da rede do Banco, informações consolidadas (analíticas e sintéticas) com resultados de trabalhos de auditoria.

PERGUNTA 37:

Entendemos que se o sistema possibilitar a geração de relatórios esse item estará atendido, visto que a gravação em mídia externa ou a impressão cabe ao usuário da solução. Nosso entendimento está correto?

RESPOSTA:

A gravação de dados em mídia removível é para atender a necessidade da Auditoria de enviar informações ao público externo. Algumas dessas informações podem ser em formato de relatório e outras não. Poderá ser necessário, por exemplo, fornecer informações em uma visão de árvore para o Comitê de Auditoria.

ITEM 3.171:

O sistema terá que emitir relatório com informações consolidadas sobre o resultado dos trabalhos de auditoria, com *layout* customizável, para reporte ao Conselho de Administração, Conselho Fiscal, Comitê de Auditoria e outros órgãos demandantes.

PERGUNTA 38:

O que deve ser customizável no layout? O que se deseja seria um gerador de relatórios de mercado?

RESPOSTA:

Modelos diferenciados de relatórios a serem definidos pela Área de Auditoria que possam ser emitidos a partir do sistema.

ITEM 3.183:

O sistema terá que controlar a realização da avaliação da qualidade de trabalho, emitindo alertas quanto ao atraso de procedimentos.

PERGUNTA 39:

Deverá se emitido alerta quando houver atraso em qual procedimento? Procedimento de avaliação do trabalho ou procedimento de auditoria?

RESPOSTA:

Quando houver atraso no procedimento de avaliação do trabalho.

ITEM 3.201:

O sistema terá que permitir cadastrar e acompanhar os fluxos para acompanhamento das recomendações de auditoria.

PERGUNTA 40:

Entendemos que o registro de manifestações pela auditoria e pelas áreas auditadas atenderia a esse item. Nosso entendimento está correto? Se nosso entendimento não estiver correto, o que devemos entender como “fluxos para acompanhamento de recomendações de auditoria”? Gentileza exemplificar.

RESPOSTA:

A depender da criticidade das ocorrências e da unidade responsável pelo atendimento à recomendação da auditoria poderá haver diferença no fluxo das solicitações de repactuação de prazos de recomendações, em relação ao envolvimento de alçadas superiores. Já com relação ao fluxo de baixa de recomendação, o fluxo é único.

ITEM 3.240:

O sistema terá que permitir definir o fluxo para acompanhamento dos diferentes tipos de demandas de órgãos de controle e fiscalização e de auditoria independente, com os responsáveis por cada etapa, as ações envolvidas e as situações possíveis, a partir de catálogo de situações mantido pelo aplicativo (exemplo: vincenda, vencida, a certificar, certificada, prejudicada, aguardando manifestação do órgão externo, a certificar por órgão externo, certificada por órgão externo).

PERGUNTA 41:

O que devemos entender como “definir fluxos para acompanhamento de diferentes tipos de demanda de órgãos de controle e fiscalização...”? Gentileza exemplificar

RESPOSTA:

O fluxo corresponde à seqüência de ações com os respectivos responsáveis, ou seja, o trâmite dos encaminhamentos desde o início até o final de uma demanda. A depender da classificação do tipo de demanda, o fluxo poderá ser distinto.

ITEM 3.254:

A solução terá que possuir módulo gerador de relatórios para permitir a criação de relatórios sintéticos e analíticos, por painéis, gráficos e mapas dinâmicos, com layout customizável e definição de filtros para a recuperação de informações.

PERGUNTA 42:

- a) O que se deseja é um aplicativo gerador de relatórios de mercado, como por exemplo: Crystal Reports, Jasper Reports, Reporting Services da Microsoft, entre outros?
- b) O que se pede nesse item seria um módulo de georeferenciamento de mercado? Se sim, seria apenas uma base de mapas para plotagem de indicadores e informações gerenciais? Se não, gentileza esclarecer o que seria “mapas dinâmicos” e exemplificar.

RESPOSTA:

Está correto o entendimento da empresa, mas a solução não está limitada aos produtos por ela citados. O termo mapa dinâmico não se refere a módulo de georeferenciamento de mercado, mas sim a indicadores e informações gerenciais.

ITEM 3.256:

A solução terá que permitir pesquisar palavras-chaves nos arquivos anexos vinculados aos diversos cadastros mantidos pelo aplicativo (exemplo: documentos do Microsoft Office, BrOffice, PDF).

PERGUNTA 43:

O atendimento desse item depende do tipo de solução que será adotada pelo BNB para armazenamento de arquivos anexos. A título de exemplo, nós implantamos armazenamento de arquivos e relatórios de forma integrada com a solução de GED Content Manager da IBM, e isso tornou possível realização das pesquisas solicitadas. Em outra implantação, os arquivos foram armazenados em campos blob do banco de dados, o que não possibilitou a pesquisa. Gentileza esclarecer qual seria a estrutura de armazenamento de arquivos anexos e relatórios a se utilizada pelo BNB.

RESPOSTA:

Estes arquivos anexos não serão mantidos na aplicação a ser adquirida? Não podemos definir o meio de armazenamento da solução se isso está a cargo de cada fornecedor.

ITEM 3.260:

O sistema terá que notificar a Área de Controles Internos, Segurança e Gestão de Riscos sobre as fragilidades identificadas nos trabalhos de auditoria, de acordo com sua criticidade e abrangência, com os respectivos fatores de risco, causas e conseqüências, para avaliação e classificação dos riscos por aquela Área.

PERGUNTA 44:

Como seria essa notificação? Por e-mail, pelo portal ou por emissão de relatório específico para essas áreas? Essas áreas teriam acesso ao sistema da auditoria?

RESPOSTA:

Algumas informações poderão ser trocadas por meio de interface entre os sistemas e outras disponibilizadas no portal de auditoria. Essa área precisa ter acesso com perfis diferenciados ao nosso sistema.

Fortaleza, 18 de agosto de 2010.

Pelo BANCO DO NORDESTE DO BRASIL S.A.

Geórgia Maria Leite Sydrião Ferreira
Gerente de Célula de Auditoria, em exercício

