

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA
Curso Segurança da Informação

Brian Udson Gonsales

SEGURANÇA EM ERP SAP
Controle de Acesso via SAP GRC Access Control

Americana, SP

2014

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

Brian Udson Gonsales

SEGURANÇA EM ERP SAP

Controle de Acesso via SAP GRC Access Control

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Segurança da Informação, sob a orientação da Prof.^a Me. Graziela Rocha Reghini Ramos

Área de concentração: Controle de Acesso.

Americana, S. P.

2014

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

G645s	Gonsales, Brian Udson Segurança em ERP SAP: controle de acesso via SAP <i>GRC Access Control.</i> / Brian Udson Gonsales. – Americana: 2014. 66f. Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza. Orientador: Prof. Me. Graziela Rocha Reghini Ramos 1. Sistemas de informação I. Ramos, Graziela Rocha Reghini II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.
-------	---

CDU:681.518

Brian Udson Gonsales

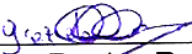
SEGURANÇA EM ERP SAP

Controle de Acesso via SAP GRC Access Control

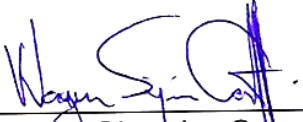
Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnóloga em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Controle de Acesso.

Americana, 4 de dezembro de 2014.

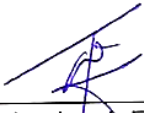
Banca Examinadora:



Graziela Rocha Reghini Ramos (Presidente)
Mestre em Linguística
Fatec Americana



Wagner Siqueira Cavalcante (Membro)
Mestre em Ciência da Computação
Fatec Americana



Clerivaldo José Roccia (Membro)
Mestre em Tecnologia
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar à Prof.^a Graziela Ramos por ter graciosamente me aceitado como um de seus orientandos e ter me provido recursos mais que suficientes para que este trabalho fosse concretizado.

À coordenadora Maria Cristina Luz por ter me provido condições de ingressar na disciplina de TCC, apesar de minhas limitações.

A todo o quadro de funcionários da FATEC Americana cujo empenho foi vital no meu desenvolvimento no mercado de trabalho.

RESUMO

Num mercado corporativo cada vez mais competitivo, a integridade nas atividades financeiras deixou de ser um diferencial para tornar-se um requisito indispensável para a sobrevivência das empresas de capital aberto. À luz da grande demanda por segurança e confiabilidade nos negócios, o peso da responsabilidade recai sobre os sistemas de informação – especificamente sobre seus administradores e gestores de segurança, que necessitam de soluções cada vez mais inovadoras para gerir grandes sistemas com agilidade, disponibilidade e segurança. Este cenário é contextualizado, ao longo deste trabalho, em um dos maiores softwares empresariais integrados da atualidade, o sistema de informação para grandes empresas, chamado de *SAP*. Discutem-se ainda os desafios apresentados na sua gestão em larga escala, assim como a introdução, feita pelo próprio fabricante, de um conjunto de ferramentas utilizado para viabilizar a gestão segura de seus sistemas, chamados de *SAP GRC*, especificamente no que se refere às atividades de controle de acesso. Por fim, um estudo é realizado de modo a levantar o nível de satisfação real que é obtido em sistemas *SAP* geridos através do *SAP GRC*, assim como seus benefícios e potenciais pontos de melhoria.

Palavras Chave: controle de acesso, sistemas de informação, ERP, SAP, GRC.

ABSTRACT

In a competitive corporate environment, financial integrity is no longer a desired quality, but a regulatory requirement, strictly needed for companies that wish to remain active on the market. The weight of financial integrity befalls upon the companies' information systems – specifically upon their administrators and security managers, who are in constant need of innovative solutions to aid them in performing their tasks, so that the information systems are always readily available and secure. In this paper, a scenario is presented within one of the biggest enterprise software to the present, the integrated information system known as SAP. A discussion is raised around the present challenges in a large-scale SAP security system management, as well as the introduction of the SAP-delivered package solution for secure system management known as SAP GRC, as far as access control is concerned. Lastly, a field research is provided in order to evaluate the overall customer satisfaction levels about issues related to access control with the SAP GRC solution and to identify its biggest benefits and potential points for improvement.

Keywords: *access control, information systems, ERP, SAP, GRC.*

SUMÁRIO

AGRADECIMENTOS	i
RESUMO	ii
ABSTRACT	iii
SUMÁRIO	iv
LISTA DE ABREVIATURAS E SIGLAS	vi
LISTA DE FIGURAS E DE TABELAS	vii
1 INTRODUÇÃO	11
2 SOFTWARES ERP	13
2.1 SEGURANÇA EM AMBIENTES ERP	15
3 O ERP SAP	18
3.1 O CONCEITO DE AUTORIZAÇÃO SAP	21
4 CONTROLE DE ACESSO NO SAP	25
5 O CONTROLE DE ACESSO E O MERCADO	28
6 SAP GRC	32
7 GRC ACCESS CONTROL	35
7.1 ACCESS REQUEST MANAGEMENT (ARM)	36
7.2 ACCESS RISK ANALYSIS (ARA)	39
7.3 BUSINESS ROLE MANAGEMENT (BRM)	44
7.4 EMERGENCY ACCESS MANAGEMENT (EAM)	46
8 ESTUDO DE MERCADO	49
9 ANÁLISE DE RESULTADOS	50
10 CONSIDERAÇÕES FINAIS	52
REFERÊNCIAS BIBLIOGRÁFICAS	55
ANEXO A – MATRIZ DE PAPÉIS E RESPONSABILIDADES DO ARA	58
ANEXO B – QUESTIONÁRIO	60
ANEXO C – GRÁFICOS DE RESULTADOS DO QUESTIONÁRIO	62

ANEXO D – GLOSSÁRIO.....65

LISTA DE ABREVIATURAS E SIGLAS

Termo	Definição
ABAP	<i>Advanced Business Application Programming</i>
AC	<i>Access Control</i>
ARA	<i>Access Risk Analysis</i>
ARM	<i>Access Request Management</i>
BRM	<i>Business Role Management</i>
CRM	<i>Client Relationship Management</i>
EAM	<i>Emergency Access Management</i>
ECC	<i>Enterprise Central Component</i>
ERP	<i>Enterprise Resource Planning</i>
GRC	<i>Governance, Risk & Compliance</i>
SAP	<i>Systems, Applications & Products</i>
SOx	<i>Sarbanes-Oxley</i>

LISTA DE FIGURAS E DE TABELAS

Tabela 1 – Exemplo de Matriz de Funções.....	39
Figura 1 – Ambiente de sistemas heterogêneos.....	14
Figura 2 – Ambiente integrado através de software ERP.....	14
Figura 3 – Pesquisa de Campo da PricewaterhouseCoopers.....	16
Figura 4 – Incidentes de segurança da informação dentro dos 12 últimos meses.....	17
Figura 5 – Principais agentes causadores de incidentes de segurança da informação.....	17
Figura 6 – Arquitetura Cliente/Servidor do SAP.....	19
Figura 7 – Exemplo de Transação/T-code.....	22
Figura 8 – Composição das Roles dentro de um perfil de usuário.....	23
Figura 9 – Kenneth Lay na manchete do jornal The New York Post, 26 de maio de 2006.....	29
Figura 10 – Investidores em relação a empresas com boa e má governança....	31
Figura 11 – Interação entre as três disciplinas do GRC.....	34
Figura 12 – Nomenclatura dos componentes do GRC AC.....	35
Figura 13 – Funções como parte de um Risco.....	40
Figura 14 – Regras, Funções e Riscos como parte do Rule Set.....	41
Figura 15 – Exemplos de Metodologias de Manutenção.....	45

1 INTRODUÇÃO

Com o advento dos sistemas de informação integrados, os processos internos das empresas mais competitivas do mercado vêm tomando novas dimensões. Da manufatura à venda, a cadeia de processos pode ser toda processada por um único sistema, no qual se concentram todos os tipos de informação. De informações técnicas de composição do produto e dados de estoque até preços e dados sobre vendas e distribuição – todas essas informações convenientemente armazenadas em uma única base de dados, prontas para serem utilizadas da maneira mais eficiente possível.

Em contrapartida deste grande passo no ramo dos sistemas de informação, a questão da segurança da informação cresce em número e importância. De acordo com a pesquisa global *The Global State of Information Security® Survey 2015* realizada pela PricewaterhouseCoopers em maio de 2014¹, os incidentes relacionados segurança de informação cresceram 48% em relação a 2013. Tais dados nos levam a questionar: existem leis regulamentadoras que exijam níveis aceitáveis de segurança em sistemas de informação? Como manter todos os dados seguros num ambiente de sistema de informação cada vez mais complexo? As soluções de segurança existentes satisfazem as necessidades dos clientes?

Este trabalho leva em conta o cenário ocorrente em um dos maiores sistemas de informação integrado do tipo ERP (*Enterprise Resource Planning*) existentes, o SAP (*Systems, Applications & Products*). O objetivo geral é descrever e definir a solução que o fabricante oferece para gestão segura de seus sistemas, chamada de SAP GRC (*Governance, Risk and Compliance*), apontar suas principais soluções e metodologias, definir seus casos e possíveis aplicações e, por fim, avaliar se a solução satisfaz as necessidades que as empresas do mercado têm atualmente.

Após a introdução do assunto neste primeiro capítulo, o capítulo dois introduz e explana o conceito de software ERP. Já o terceiro capítulo aborda especificamente o software ERP da SAP. O quarto capítulo apresenta o conceito de autorização do ERP SAP, enquanto que o quinto relata acontecimentos no mercado que evidenciaram a

¹ Disponível em: <http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml#>. Data de acesso: 13 de outubro de 2014.

questão da segurança da informação no contexto de software ERP. O sexto capítulo apresenta a resposta da SAP à questão da segurança, através de um pacote de aplicações chamado SAP GRC, enquanto que o sétimo estuda a fundo a solução criada para a questão do controle de acesso. O oitavo capítulo reserva-se à uma pesquisa de mercado realizada através de questionário de perguntas fechadas para avaliar a satisfação do mercado em relação a solução criada pela SAP e o capítulo nove à análise e interpretação dos resultados da pesquisa. Por fim, o décimo capítulo traz as observações finais e considerações acerca do estudo.

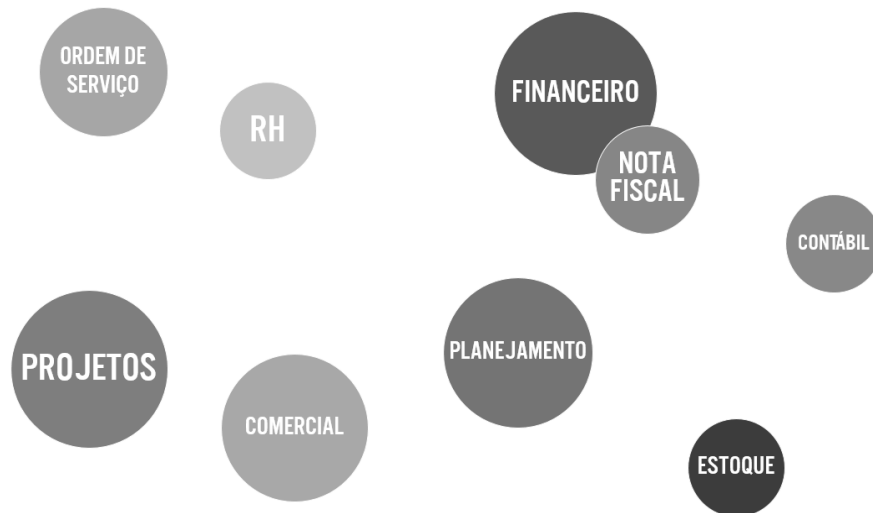
2 SOFTWARES ERP

No mercado atual, as grandes corporações têm buscado algum tipo de integração de seus sistemas de informação. Uma pesquisa conduzida em 2013 pelo instituto *ACM Computing Surveys* (Shaul et al, 2013) revela que, na última década, mais de 80% das grandes empresas dos EUA já investiram em integração e aproximadamente um terço delas citaram ou ainda citam integração como um dos investimentos prioritários no ramo de TI – o que impulsiona a procura de mercado por um sistema integrado de gestão empresarial. Tal sistema é conhecido atualmente como ERP.

O ERP (do inglês *Enterprise Resource Planning*, também chamado de Sistemas Integrados de Gestão Empresarial) é um conjunto de sistemas de informação que tem como função integrar dados e processos de uma organização em um único pacote de aplicações. Em termos gerais, o ERP é responsável por integrar as operações dos diversos departamentos de uma empresa utilizando fluxos integrados de automação de processo que rodam sob uma plataforma unificada.

Segundo Alecrim (2010), grande parte dos ERPs disponíveis no mercado atualmente opera de maneira modular. Tais módulos podem ser divididos dentro da perspectiva *funcional* ou *técnica*. A primeira diz respeito à gestão das operações de negócio em si, enquanto a última é relacionada ao universo tecnológico e tem como objetivo o suporte das aplicações que operam dentro da perspectiva *funcional*. Finanças, contabilidade e recursos humanos podem ser citados como exemplos de módulos que operam sob o ponto de vista *funcional*, enquanto que monitoramento de performance, administração de servidores e gestão de segurança são exemplos de módulos *técnicos*, os quais são responsáveis por manter o pleno funcionamento dos módulos *funcionais*, através da manutenção e configuração do próprio sistema ERP em seu âmbito técnico.

Ilustrando um cenário de integração, a figura 1 representa um ambiente em que existem vários sistemas separados para cada finalidade.

Figura 1 – Ambiente de sistemas heterogêneos

Fonte: próprio autor

O papel da integração via ERP é converger todos os sistemas, mas ainda mantê-los coexistindo de maneira modular, sob uma única plataforma, conforme ilustrado pela figura 2.

Figura 2 – Ambiente integrado através de software ERP

Fonte: próprio autor

2.1 SEGURANÇA EM AMBIENTES ERP

Van Holsbeck (2004) afirma que a contínua integração oferecida pela plataforma ERP, embora benéfica e vantajosa, também potencializa o impacto financeiro de uma invasão ou fraude – uma vez que múltiplas funções e recursos da companhia se encontram concentradas numa única plataforma. Um exemplo comum de novas brechas de segurança abertas pela própria natureza concentradora do sistema se dá no âmbito da cadeia integrada de suprimentos (também chamada de “Supply Chain Management”, ou *SCM*), onde um fornecedor é integrado ao sistema para que o fluxo de suprimentos seja executado de forma contínua. Embora de grande valia ao funcionamento do *SCM*, tal ação também abre uma nova porta para que o sistema seja explorado ou fraudado por um terceiro, que passa de uma simples entidade externa a assumir o papel de usuário ativo no sistema ERP, assim ganhando acesso a um perímetro de segurança outrora inacessível.

Essas e outras peculiaridades levam a administração de segurança no meio ERP corporativo a pensar de forma diferenciada, não somente focada nas proteções de perímetro, mas também levando em conta os riscos financeiros provenientes de fraudes. Van Holsbeck também comenta que, embora uma grande parte dos esforços da equipe de segurança se voltem à proteção de perímetro, o real potencial de perda ou fraude financeira se concretiza através de usuários que já estão dentro do sistema.

Como frisado por Shaul e Tauber (2013), a questão da segurança nos ERPs somente vem ganhando importância nos últimos anos desta década. Embora os provedores de ERP estejam focados em desenvolver novas funcionalidades (como *CRM* e *Web Services*) para adicionar valor aos seus produtos primários, a segurança nesse contexto não estava entre as prioridades desde o início – o que levou os provedores de ERP a reverem os conceitos de segurança dos seus produtos ou desenvolverem produtos adicionais para garantir a gestão segura dos seus ERPs:

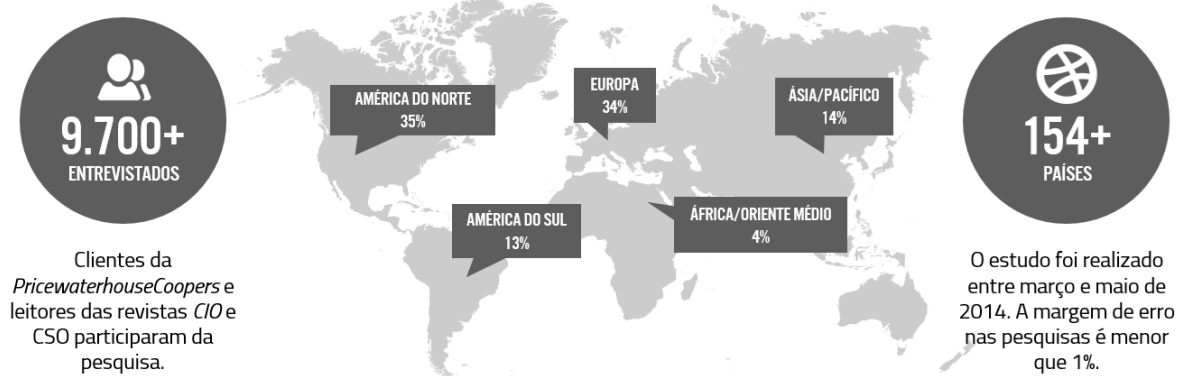
“The ERP market has matured to a point where heightened competition has brought declining sales. As a result, ERP vendors are committed to bundling new functionality, such as CRM and Web services-based architecture, to provide more value to their customers. Unfortunately, security remains an afterthought.” (Van Holsbeck, 2004, p. 1)

Tradução: “O mercado ERP amadureceu ao ponto onde a elevada competição trouxe consigo o declínio das vendas. Como resultado, os distribuidores de ERP se focaram em atrelar novas funcionalidades, assim como CRM e Web Services pra agregar mais valor a seus

consumidores. Infelizmente, a segurança ainda continua em segundo plano.”

Corroborando o ponto de vista apresentado por Shaul e Tauber, o grupo *PricewaterhouseCoopers*, em parceria com as revistas *CIO* e *CSO*, realizou uma pesquisa no campo da segurança da informação. Os entrevistados foram empresas do mundo todo, de acordo com a Figura 3. As entrevistas ocorreram entre março e maio de 2014.

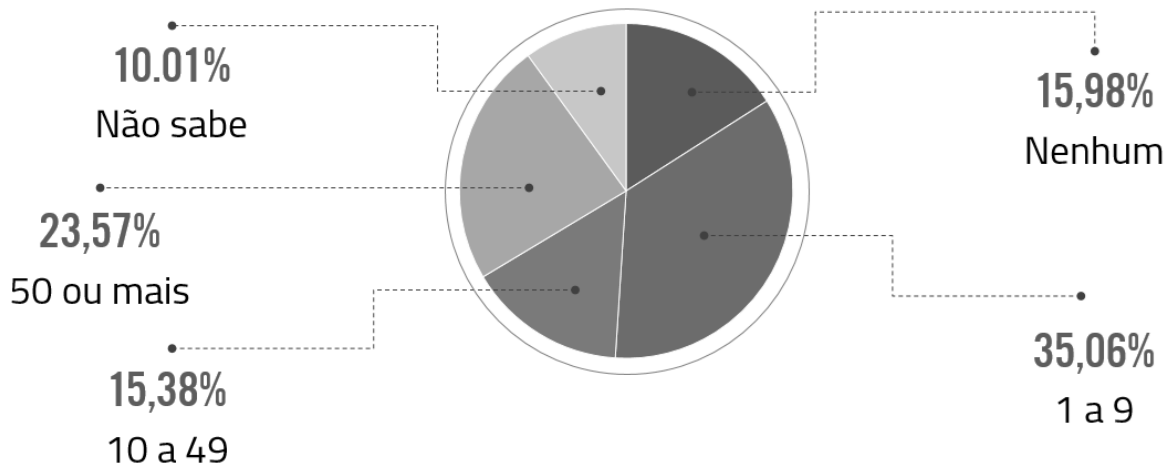
Figura 3 – Pesquisa de Campo da *PricewaterhouseCoopers*



Fonte: próprio autor

A pesquisa revela que aproximadamente 23% dos entrevistados sofreram mais de 50 incidentes de segurança da informação dentro dos últimos 12 meses, conforme figura 4.

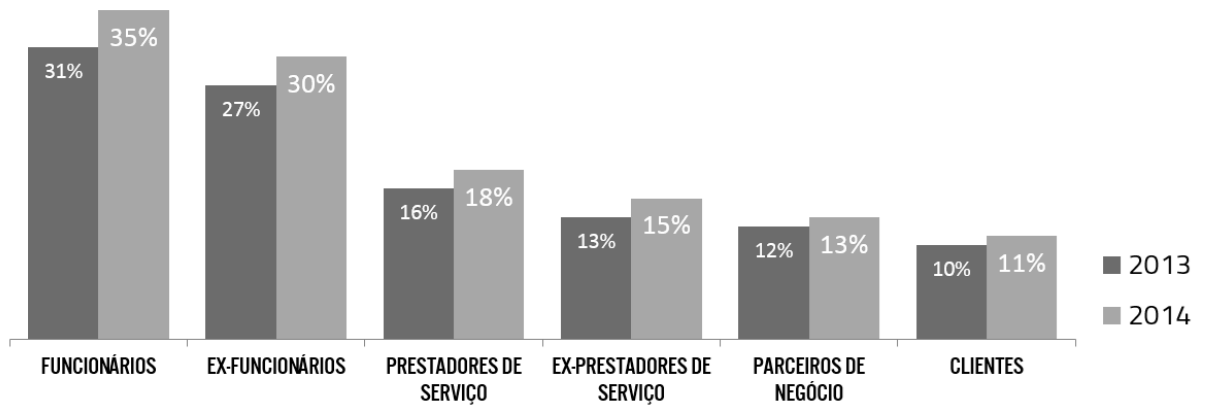
Figura 4 – Incidentes de segurança da informação dentro dos 12 últimos meses



Fonte: próprio autor

A pesquisa também revela que os agentes causadores mais citados são os próprios funcionários da empresa, conforme figura 5.

Figura 5 – Principais agentes causadores de incidentes de segurança da informação



Fonte: próprio autor

3 O ERP SAP

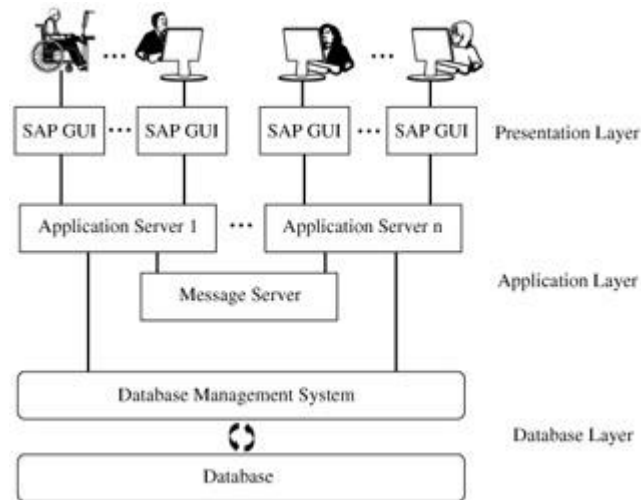
Tido atualmente como o ERP líder de mercado, o SAP ERP (atualmente chamado de SAP ECC – *Enterprise Central Component*),⁰ é o carro-chefe da fabricante de software corporativo multinacional SAP SE. Com sede em Walldorf, Alemanha, a SAP SE lidera o mercado de ERPs corporativos com um faturamento de € 14.16 bilhões, 64.598 empregados e aproximadamente 25% do mercado mundial de ERP, segundo seu relatório financeiro de 2013 e o censo de maio do mesmo ano, realizado pelo grupo Forbes – sendo assim não somente a maior fornecedora de ERPs, mas também uma das maiores companhias de software do mundo atual. Além do ECC, a SAP também é notável por oferecer produtos na área de *Business Intelligence*, CRM, SCM, e da mais recente plataforma de computação em memória, o SAP HANA.

O SAP opera numa arquitetura cliente/servidor de três camadas, o que originou o termo “SAP R/3” – sendo o “R” de “*Real Time*” ou processamento em tempo real, e o “3” por funcionar num modelo de 3 camadas cliente-servidor. Mais tarde, a nomenclatura “R/3” cedeu e o SAP passou a ser chamado “SAP ERP” (Kogent, 2010, p. 3).

Todos os dados são armazenados num banco de dados único e são processados na camada de aplicação dos servidores de aplicação. A camada de apresentação do *front-end*, chamada de *SAPgui*, é responsável pela interface com o usuário.

A figura 6 mostra uma representação gráfica da arquitetura cliente/servidor do SAP.

Figura 6 – Arquitetura Cliente/Servidor do SAP



Fonte: Kogent, 2010, p. 7

Kogent (2010) descreve as camadas da seguinte maneira:

- **Camada de Apresentação (*Presentation Layer*):** além de prover a interface gráfica com o usuário através do *SAP GUI (Graphical User Interface)*, a camada também é utilizada para a entrada e visualização de dados. Esta recebe os dados fornecidos pelo usuário, envia-os para a camada de Aplicação. A resposta é então recebida e repassada ao usuário final.
- **Camada de Aplicação (*Application Layer*):** a camada de aplicação provê a interface entre a camada de Apresentação e a Camada de Base de Dados. Ela é também responsável por interpretar a linguagem de programação e gerenciar entrada e saída de dados. O interpretador se inicia quando o servidor de aplicação é ligado e se finaliza quando o servidor é desligado.
- **Camada de Base de Dados (*Database Layer*):** um banco de dados centralizado que contém todos os dados no sistema SAP ERP. Esta camada recebe os pacotes da camada de Aplicação e os repassa ao sistema de gerenciamento de banco de dados relacional, que envia os dados requisitados de volta ao servidor de aplicação.

Segundo Hirao et al (2009, p. 34), na camada de Apresentação, o sistema oferece, nativamente, um processo de autenticação através de combinação de usuário e senha. As políticas podem ser definidas pelo administrador do sistema e mudadas de acordo com a necessidade do negócio. Hirao também mostra que, como medidas de segurança adicionais ao processo de autenticação, também é possível elencar os seguintes elementos:

- SNC (*Secure Network Communication*): integra um serviço de segurança externo ao SAP, adicionando métodos de autenticação não suportados nativamente pelo SAP. Uma vez verificado e homologado pelo SSPP (*SAP Software Partner Program*), o SNC disponibiliza funções para verificação de identidade, proteção de integridade, ou serviços de proteção de privacidade.
- SSL (*Secure Sockets Layer*): o serviço de SSL pode ser integrado ao SAP, provendo encriptação de dados e autenticação no nível de cliente e/ou servidor, transportando os dados de autenticação de maneira segura pela rede. Conexões HTTP seguras também podem ser realizadas como o SSL.
- Certificados X.509: sendo utilizado de maneira similar ao SSL, o X.509 provê certificados de autenticação que podem excluir a necessidade de se utilizar usuário/senha, se assim configurado. Como parte da infraestrutura de Chaves Públicas (PKI), o usuário que deseja acessar o sistema apresenta seu certificado utilizando os protocolos SSL. Somente o servidor consegue descriptografar essa requisição de *login*, e verifica a existência do usuário dentro do sistema SAP. Caso o *login* seja verificado com sucesso, o processo de autenticação se dá através dos protocolos SSL inclusos, excluindo a necessidade de entrada manual de usuários/senhas.

Uma vez autenticada a sessão de login do usuário, a próxima camada de segurança presente no sistema se dá na camada de Aplicação, onde se utiliza o conceito de autorização comum a todas instâncias SAP.

3.1 O CONCEITO DE AUTORIZAÇÃO SAP

Antes de adentrar-se o tema do conceito de autorização em si, é importante que a contextualização seja feita acerca da linguagem de programação e da arquitetura utilizada num servidor de aplicação SAP.

De Bruyin e Lyfareff (1998) descrevem o ABAP (*Advanced Business Application Programming*, originalmente *Allgemeiner Berichts-Aufbereitungs-Prozessor*, ou "processador de criação de relatórios genéricos") como uma linguagem de programação de alto nível utilizada em todos os sistemas SAP. Sendo parte do grupo de linguagens de programação de quarta geração, o ABAP é totalmente específico às aplicações SAP. Os autores também comentam que o ABAP é a linguagem utilizada pela SAP para a criação da plataforma SAP ERP e é comumente usada pelos clientes para ampliar as funcionalidades dos programas ou customizar certos trechos do código padrão, evitando o esforço de criar programas do zero e utilizando os recursos já existentes para construir soluções customizáveis e adaptadas às necessidades do negócio.

Todas as aplicações do SAP são, essencialmente, programas codificados através do ABAP. A porta de entrada às aplicações criadas com o ABAP, sejam elas padrões ou customizadas, são denominadas códigos de transação, ou *T-Codes*, as quais podem ser acessadas através do campo de comando, localizado no canto superior esquerdo da tela, ou do *Area Menu*, presente no formato de uma barra de navegação do no lado esquerdo da tela inicial.

Figura 7 – Exemplo de Transação/T-code

Enter G/L Account Document: Company Code 1000

Tree on Company Code Hold Simulate Park Editing options

Basic data Details

Document Date Currency EUR

Posting Date 10/17/2010

Reference

Doc. Header Text

Document Type SA G/L account posting

Cross-CC no.

Company 1000 IDES Inc Philadelphia

Amount Information

Total deb. 0.00 EUR

Total cred. 0.00 EUR

0 Items (No entry variant selected)

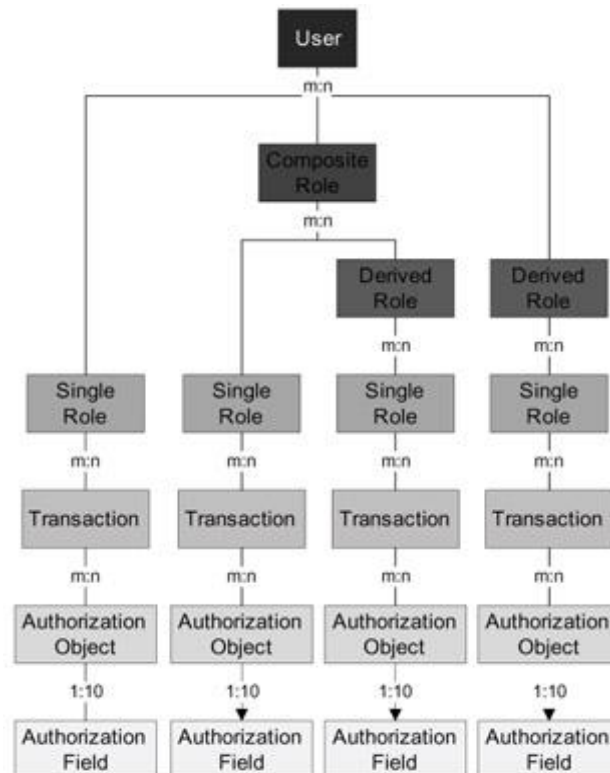
St	G/L acct	Short Text	D/C	Amount in doc.curr.	Loc.curr.amount	T	Tax jurisdictn code	Assignment no.
					0.00			
					0.00			
					0.00			
					0.00			
					0.00			
					0.00			
					0.00			
					0.00			
					0.00			
					0.00			

Fonte: próprio autor

Hirao et al (2009) afirma que, para acessar as *T-codes*, um usuário precisa conter as autorizações corretas atribuídas a seu perfil de usuário no SAP, as quais são definidas através de grupos de autorização, chamadas de *Roles*. As *Roles* constituem conglomerados de autorizações, preferencialmente projetadas para atender uma necessidade de negócio do usuário final, liberando acesso ao sistema de maneira gradual, e evitando que este ganhe acesso a áreas críticas ou que não possuem relação com as funções de trabalho do mesmo.

A figura 8 mostra a relação hierárquica das *Roles* e o usuário no sistema SAP.

Figura 8 – Composição das Roles dentro de um perfil de usuário



Fonte: Hirao et al, 2009, p 36.

Hirao et al (2009) descreve cada elemento da seguinte maneira:

- *Authorization Field* (Campo de Autorização): constituindo o nível mais baixo da estrutura hierárquica de autorização, o *Authorization Field* corresponde a um campo no banco de dados definido pela estrutura ABAP. Estes campos são o alvo de atuação da estrutura de autorização, onde se definem a quais campos o usuário terá acesso.
- *Authorization Object* (Objeto de Autorização): o Objeto de Autorização é um conjunto de Campos de Autorização, de modo a criar um perfil compreensivo de acesso para cada processo e subprocesso de negócio. Um Authorization Object define quais campos e qual o nível de acesso (criação, modificação, visualização) disponível para cada conjunto lógico de campos. Tanto o nível de acesso quanto os campos de cada Objeto de Autorização podem variar de acordo com cada processo, subprocesso ou contexto lógico, compondo assim um ambiente de autorizações flexível, adaptativo e escalável.

- *Transaction* (Transação): cada Transação SAP contém uma lista nativa de checagem de Objetos de Autorização, que compõem seus requisitos mínimos de acesso. Esta lista, porém, pode ser customizada pelo cliente, de modo a definir quais Objetos de Autorização serão checados em tempo de execução. Objetos de Autorização criados pelo cliente também podem ser introduzidos
- *Role*: as *Roles* são conjuntos de Transações de Objetos de Autorização, que são por fim atribuídas aos usuários pelo administrador do sistema ou equipe de segurança. Elas podem ser *Roles* simples (*Single Roles*), compostas (*Composite Roles*) ou derivadas (*Derived Roles*).
 - *Single Roles*: o tipo mais básico de *Role*, que contém um conjunto de autorização denominado e um único perfil de *Role* é gerado.
 - *Derived Roles*: consistem de *Single Roles* dentro de um mesmo modelo, mas que diferem em alguns campos de autorização chave. Muito comumente usadas para criar *roles* para o mesmo cargo, mas localizações geográficas distintas. Elas podem ser criadas para o cargo de analista contábil, porém com uma derivação para o Brasil e outra semelhante derivada especificamente para o México.
 - *Composite Roles*: chama-se de *Composite Role* o agrupamento de duas ou mais *Roles*.

De acordo com as notas do fabricante, o conceito de autorização do SAP é construído de forma a viabilizar o *Princípio do Privilégio Mínimo*, em que um usuário, quando criado, não possui acesso a função alguma dentro do sistema. Esse só passará a possuir privilégios no momento em que o administrador ou equipe de segurança atribui as *Roles* ao seu perfil. O conceito de atribuição de *Roles* é aditivo, ou seja, não existem *Roles* que reduzam o acesso ou privilégios do usuário que as possui.

Uma vez conhecido o conceito de autorização utilizado pelo ERP SAP, a seção a seguir demonstrará as utilizações típicas do controle de acesso ao sistema, utilizando-se das ferramentas que o SAP provê nativamente, assim como a descrição dos principais desafios na gestão de um ambiente ERP SAP.

4 CONTROLE DE ACESSO NO SAP

Sabendo-se que o ABAP é uma linguagem de alto nível voltada a negócio, é de comum conhecimento que os seus Objetos de Autorização também são voltados diretamente a este propósito, permitindo assim que as *Roles* atendam às necessidades de um denominado cargo, localidade ou contexto. Portanto, é de grande importância que todas as *Roles* do sistema sejam desenhadas de maneira flexível, escalável e que se adapte às peculiaridades da empresa.

Enquanto a adaptabilidade das permissões e privilégios evolui, o controle de acesso também deve progredir em proporcional escala. Proteger os processos corporativos e evitar o conflito de segregação de funções (comumente chamados de *SoD* ou *Segregation of Duties*) é primordial para o estabelecimento de um ambiente SAP seguro.

Um exemplo clássico de conflito de segregação de funções (também chamado *SoD conflict*) se dá num cenário onde um certo usuário do sistema SAP possui acesso às seguintes funções:

1. *Criar fornecedor (T-code XK01)*
2. *Realizar pagamentos a fornecedor (T-code F110)*

Dessas duas funções conflitantes se origina o conflito de segregação de funções, no qual se apresenta o risco de que um fornecedor falso seja criado pelo usuário e que o mesmo efetue pagamentos fraudulentos a este fornecedor.

À luz dos riscos que os conflitos de segregação de função representam à corporação, os desafios no controle de acesso se apresentam em várias frentes, como descrito a seguir.

As *Roles*, se desenhadas de forma muito ampla e permissiva, irão reduzir o esforço necessário para implementá-las e atenderão facilmente às necessidades dos usuários – porém o risco de *SoDs* aumentará significativamente. Por outro lado, se as *Roles* forem projetadas de forma excessivamente restritiva ou fragmentada, o esforço de implementação será maior, ao passo de que os conflitos de *SoD* serão mínimos e mais fáceis de serem resolvidos. O ideal é que um equilíbrio seja alcançado entre restrições e permissões, condizentes com o contexto do sistema em questão,

resultando em *Roles* que são ao mesmo tempo adequadas ao perfil de cada usuário e que proporcionem um ambiente seguro e livre de conflitos de segregação de funções.

O desafio neste processo se dará no momento de definir papéis e responsabilidades de todos os usuários envolvidos. Além de um bom levantamento de micro e macro funções, os analistas de segurança e representantes das áreas funcionais devem trabalhar juntos para transformar os requerimentos em perfis de acessos coerentes, prevendo casos de ampliação ou redução de funções, evitando assim futuros problemas decorrentes de má estruturação das *Roles* – o que leva um longo tempo pra ser resolvido, por envolver grandes quantidades de retrabalho, além de uma readaptação do conceito inicial (Labadessa et al, 2013).

Uma vez desenhadas e devidamente definidas, as *Roles* passam a ser atribuídas aos usuários de acordo com o plano. Novos usuários são criados, alterados ou removidos de acordo com as necessidades do negócio e a equipe de segurança trabalha para atender todas as solicitações de acesso em seu tempo devido.

Conforme observado pelo próprio autor em seu ambiente de trabalho, se houver, no processo, a aquisição de novas plantas ou companhias, ou o surgimento de um novo cargo por necessidade de negócio, uma análise detalhada deverá ser feita a fim de determinar se o novo requerimento já é coberto por uma combinação de *Roles* já existente. Se o cenário não for contemplado pelos perfis de acesso existentes em ambiente produtivo, uma solicitação de mudança é gerada, de acordo com as regras de *ITIL* e *Change Management*, para que uma nova *Role* seja desenhada para cobrir aquela necessidade específica.

É indispensável que os mesmos princípios e boas práticas que foram aplicadas na fase de implementação também sejam utilizados na análise da requisição e na construção da *Role*. Sgarbi (2014) destaca que não somente a equipe de segurança deve ser cautelosa na atribuição de *Roles* a usuários, mas também que cabe aos gestores possuir pleno entendimento das *Roles* sendo atribuídas aos usuários, além da responsabilidade no momento de aprovar as requisições de acesso geradas pelos mesmos.

Entretanto, em alguns casos, é impossível realizar algumas tarefas críticas ao negócio sem usufruir de acesso privilegiado em caráter extraordinário. A essa atividade dá-se o nome de gestão de usuários de alto privilégio.

Sendo um dos pontos mais críticos da operação, os usuários de alto privilégio devem estar presentes em ambiente produtivo para suportar a implementação de soluções ou a rápida resolução de incidentes que ocorrem em esferas nas quais um usuário comum tipicamente não teria acesso. De acordo com a pesquisa de mercado feita pelo grupo PwC na Bélgica em 2013², o gerenciamento de usuários de emergência ainda é um desafio para as companhias.

Sgarbi (2014) defende que o uso controlado e limitado de um usuário de alto privilégio garante flexibilidade na resolução de problemas e, ao mesmo tempo, possibilita que todas as ações sejam controladas e que os seus altos níveis de permissão não sejam utilizados para outros fins senão aqueles que foram inicialmente estipulados e aprovados.

Nativamente, o SAP não possui nenhuma solução que proporcione o monitoramento de uso de um usuário de alto privilégio de forma preemptiva. As únicas soluções eram processos de aprovação manuais em que o usuário se comprometia a utilizar somente aquilo que lhe foi previamente aprovado, mas não havia garantia de que o indivíduo por trás do usuário privilegiado não tomaria ações para seu próprio benefício, uma vez que os *logs* só podiam ser gerados algum tempo após o término da utilização do usuário.

Tal solução consiste em ativar o *log* de auditoria (disponível através da *T-code* SM19) no período em que o usuário for utilizado e confrontar os resultados com a solicitação aprovada. Este procedimento, além de tardiamente reativo, não é eficiente por si só para combater atividades fraudulentas, visto que o *log* leva certo período de tempo para ser gerado e também pode ser desativado ou alterado pelo próprio usuário em alguns casos.

² Disponível em: <http://www.pwc.be/en/publications/2013/grc-survey-belgium.pdf>. Data de acesso: 18 de outubro de 2014.

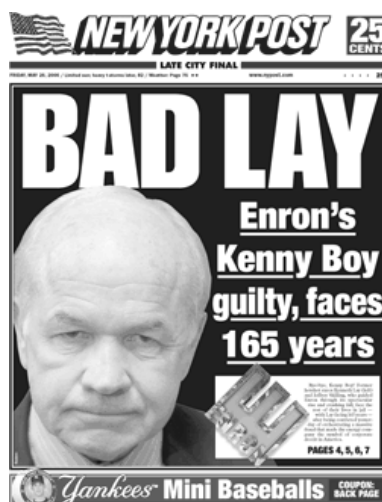
Dados estes e outros desafios apresentados nos subcapítulos anteriores, é imperativo que seja apresentada uma visão mais ampla para entender o reflexo que tais deficiências traziam no âmbito do mercado global.

5 O CONTROLE DE ACESSO E O MERCADO

Num mercado cada vez mais aquecido e competitivo, as empresas demandam uma gestão de controle de acesso cada vez mais ágil e adaptativa. Sob a pressão da competitividade, um novo desafio surge: lidar com um crescente volume de usuários por sistema, que por sua vez irá exigir cada vez mais esforço da equipe de segurança das companhias, podendo resultar em potenciais brechas causadas por erro humano ou o atraso no atendimento de solicitações críticas, que levaria a empresa a arcar com prejuízos financeiros ou com o atraso de uma agenda de negócios. Manter a gestão segura de um ambiente ERP, além de se tornar cada vez mais caro, acabava por atrasar cada vez mais os projetos, dado que a equipe de segurança enfrentava barreiras técnicas para acompanhar as rápidas mudanças estratégicas requeridas pelos clientes – um cenário bastante comum ao autor em seu ambiente de trabalho – que acabava por engessar o potencial adaptativo da companhia, ao invés de flexibilizá-lo.

Um evento marcante para o mercado da segurança de informação para sistemas de informação ocorreu entre 2000 e 2002, no caso que ficou conhecido como escândalo Enron. O grupo Enron, uma grande companhia de energia dos EUA, sofreu grande exposição na mídia, quando descobriu-se que a sua equipe de executivos não somente utilizava-se de brechas nos sistemas de informação para esconder bilhões de dólares perdidos em negociações e projetos mal-sucedidos, como também coagiram seus auditores a ignorar os rombos causados nas contas contábeis. Tanto a Enron quanto a empresa responsável por sua auditoria, a Arthur Andersen, declararam falência ao final de 2001.

Figura 9 – Kenneth Lay na manchete do jornal *The New York Post*, 26 de maio de 2006



Fonte: The New York Post

Em 2006, o fundador e CEO do grupo, Kenneth Lay, foi julgado e condenado a 45 anos de prisão. O ocorrido levou ambas as empresas a dividirem o título dado pelo estudioso William Bratton em 2002 como a “pior falha de auditoria da história”.

Motivados pelo escândalo Enron, o senador Paul Sarbanes e o deputado Michael Oxley anunciaram um projeto de lei que exigiria a criação de mecanismos de auditoria e segurança confiáveis nas empresas. O projeto também inclui regras para a criação de comitês encarregados de supervisionar atividades e operações, processos para mitigação de riscos financeiros e mecanismos de identificação de fraudes, reativas ou preemptivas, de modo a garantir a integridade de todos os relatórios financeiros gerados por empresas de capital aberto. As auditorias, que devem ser no mínimo anuais, são realizadas na base de controles pré-estabelecidos que, se violados, podem acarretar multas e, em casos extremos, a remoção da empresa da bolsa de valores ou a dissolução da mesma.

A seção 404 da Lei SOx se refere a controles internos, tendo como objetivo garantir que todas as informações processadas no sistema de informação sejam iniciadas, processadas, gravadas, armazenadas e reportadas de maneira a evitar fraudes ou qualquer outro evento que ameace a integridade dos relatórios financeiros. Para satisfazer os controles da seção 404 no contexto SAP, os seguintes pontos devem ser considerados:

- Identificar e documentar processos nos quais possíveis conflitos de segregação de função (SoD) possam existir;
- Mitigar ou eliminar os *SoDs* sempre que possível;
- Criar *Controles de Mitigação* para os *SoDs* que não possam ser mitigados;
- Elaborar *Medidas de Monitoramento* para cada *Controle de Mitigação*;
- Garantir conformidade contínua através do monitoramento dos controles.

Estes desafios, aliados à crescente visibilidade da questão de segurança na mídia levaram os clientes a aumentar ainda mais as expectativas sobre os gestores de segurança no mundo SAP ERP. Estes, por sua vez, demandavam soluções ou ferramentas mais poderosas para manter a gestão segura de seus projetos e atender às crescentes expectativas de seus clientes. O gráfico apresentado na figura 10 de uma pesquisa realizada em 2004 (dois anos após a aprovação da lei Sarbanes-Oxley), mostra que os investidores do mundo todo recompensam empresas com uma boa reputação de governança e gestão segura dos sistemas de informação, ao passo que penalizam aquelas que sofrem deficiências em seus controles internos.

Figura 10 – Investidores em relação a empresas com boa e má governança

Investors Reward Good Governance... and Penalize Poor Governance

Investors worldwide will pay a premium of 14% or more for shares in companies with good governance.

But companies with internal controls deficiencies experienced significant declines in their market caps:

14% North America & Western Europe

25% Asia and Latin America

39% Eastern Europe and Africa

McKinsey & Co. Global Investor Survey

2004 Disclosure Examples: Company/Market Value	Disclosure	% / Mkt Cap Decline
Adecco SA \$12.6 billion Jan. 12	Company delays financial statements. Internal control deficiencies	-38% \$4.9 billion
Goodyear Tire & Rubber \$1.7 billion Feb. 11	Company has not yet completed the implementation of its plan to improve internal controls	-18% \$320m
MCI \$5.4 billion Apr. 29	Material weaknesses – lack of systematic and reliable internal controls	-17% \$935m
INVESTORS FINANCIAL \$2.9 billion Oct. 21	Material weakness discovered during review of internal controls	-16% \$475m
FLOWSERVE \$1.3 billion Oct. 27	Material weakness in internal controls; two quarterly reports overdue	-11% \$152m

Fonte: McKinsey & Co. Global Investor Survey

A resposta da SAP SE à crescente demanda dos investidores por bons índices de governança veio em forma de um novo produto dentro de seus ambientes ERP, chamada de *SAP GRC*.

6 SAP GRC

Apesar de já oferecer ferramentas de segurança nativas em seus produtos, a SAP foi impulsionada a atender a crescente demanda de mercado pela questão da segurança, que era até então deixada em segundo plano pelo mercado. Broady e Roland (2008, p. 63-64) mencionam outro fator decisivo que fez com que a SAP SE se voltasse à questão da segurança e gestão de risco: a necessidade da própria SAP SE controlar seus riscos.

O primeiro passo em direção à solução que iria ser chamada de SAP GRC (Governance, Risk and Compliance) foi iniciada em abril de 2006, no momento em que foi anunciada a aquisição da *software house* norte-americana *Virsa*. A companhia desenvolvia uma ferramenta preventiva e automatizada de controle de acesso e gestão de risco, despertando o interesse da SAP em anexá-la ao seu portfólio. Após ser aperfeiçoada e adaptada, foi lançada numa versão posterior sob o nome de SAP GRC – *Governance, Risk and Compliance*. Atualmente, o SAP GRC é a ferramenta responsável por viabilizar uma gestão segura dos produtos SAP, além de oferecer alternativas para gestão de segurança em ambientes não-SAP, desde que integrados corretamente através de conectores. Vale ressaltar também que o conceito de GRC não é exclusivo ao produto SAP GRC e que existem outras ferramentas que realizam serviços voltados a GRC no mercado – algumas delas justamente voltadas ao SAP.

Além de atender à questão da segurança, que até então era deixada em segundo plano, a SAP também introduziu os conceitos de governança, análise de risco e conformidade ao seu produto primário, integrando as soluções de segurança a um nível até então nunca alcançado pelos outros ERPs do mercado.

Dentro de cada perspectiva, as disciplinas fundamentais são:

- Governança (*Governance*): sendo um termo geral, a governança no SAP GRC compreende as diretrizes que são passadas do nível executivo ao nível operacional, através da disseminação, atualização e controle de políticas, implementação de controles internos e métodos de tomada de decisão em nível estratégico. A questão da Governança é definida como a resposta para a seguinte pergunta fundamental:

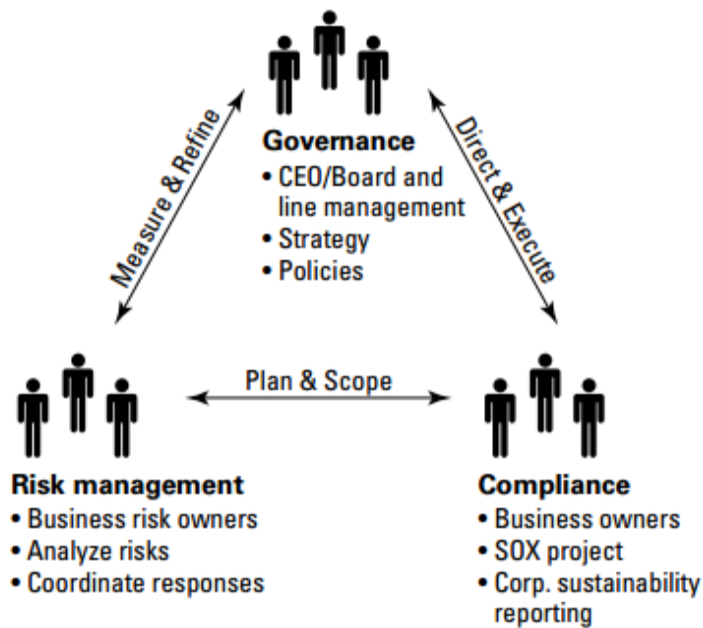
Como a alta gerência está garantindo que as suas políticas estratégicas estão sendo seguidas e através de quais meios de controle?

- Risco (*Risk*): como um dos quesitos mais abrangentes do GRC, a gestão de risco não é limitada somente ao controle de fraudes financeiras. Os riscos ambientais, tecnológicos, de mercado ou até mesmo estratégicos também são levados em conta, visto que podem causar grandes prejuízos à empresa se não mapeados e mitigados a tempo. Uma análise de risco preemptiva pode poupar a companhia de prejuízos significativos. Um caso recente de concretização de risco estratégico se deu entre a própria SAP SE e a sua maior concorrente, a Oracle. Wailgum (2009) que a SAP tinha como objetivo estratégico a migração de todos os seus sistemas para a plataforma Java até que, em 2010, a Oracle comprou a Sun Microsystems, tornando-se assim a proprietária da plataforma Java. A SAP teve de reverter seus planos de migração para a plataforma num curto período de tempo para evitar maiores danos, visto que a Oracle é a sua principal concorrente. Isso levou a SAP SE a arcar com grandes prejuízos financeiros e operacionais.
- Conformidade (*Compliance*): consiste no ato de controlar a aderência às políticas ou controles pré-estabelecidos, objetivando a eliminação de falhas de auditoria ou a minimização dos erros que levam a uma empresa a tal. Resume-se fundamentalmente no ato de cumprir controles internos e externos.

A figura 11 mostra como a interação entre as três disciplinas do GRC:

Figura 11 – Interação entre as três disciplinas do GRC

The Disciplines of GRC



Fonte: Broady & Roland, 2009, p. 24.

O pacote de aplicações do SAP GRC é composto, modularmente, pelas seguintes soluções:

- *Access Control*
- *Process Control*
- *Risk Management*
- *Global Trade Services*
- *Nota Fiscal Eletrônica*
- *Fraud Management*
- *Audit Management*

Sendo o foco deste trabalho a solução de Controle de Acesso (*Access Control*), é este que será abordado em mais detalhes na seção a seguir.

7 GRC ACCESS CONTROL

Sendo a solução de controle de acesso do GRC, o *Access Control* é utilizado para automatizar, quantificar e controlar tarefas inerentes ao cotidiano de um administrador de usuários no sistema SAP. Popularmente chamado de *GRC AC*, o pacote oferece soluções customizáveis sob vários aspectos. Estes aspectos são divididos em componentes, cujos nomes são ilustrados pela figura 12:

Figura 12 – Nomenclatura dos componentes do GRC AC

Virsa Systems	SAP GRC AC 5.3	SAP GRC AC 10
Firefighter	Super User Privilege Management	Emergency Access
Compliance Calibrator	Risk Analysis & Remediation	Access Risk Analysis
Access Enforcer	Compliant User Provisioning	Access Request Management
Role Architect	Enterprise Role Management	Business Role Management

Fonte: Boddu, 2011.

Nota-se a mudança na nomenclatura dos componentes a cada versão do pacote. Dessa maneira, é importante deixar claro que daqui em diante serão abordados os componentes da versão mais atual (SAP GRC AC 10).

7.1 ACCESS REQUEST MANAGEMENT (ARM)

Sgarbi (2013) menciona que a capacidade de criar, modificar e desligar usuários é uma das necessidades mais básicas de um sistema de informação – e ao mesmo tempo pode-se tornar uma das tarefas mais complexas de se gerenciar em larga escala. Sem as ferramentas adequadas, processar as requisições de acesso em tempo hábil e livre de erros é um desafio para os administradores de usuário, que podem levar a empresa a sofrer de interrupções de acesso, fraudes ou penalidades de auditoria causadas por erro humano no processo de atribuição de autorizações a usuários.

À luz destes cenários de risco, o *GRC Access Control* introduz o componente ARM (*Access Request Management*). O fabricante afirma que este subproduto do *GRC Access Control* é voltado a sanar tais necessidades através de um conjunto de ferramentas voltadas para automação de requisições de acesso ao sistema SAP, integrando os vários componentes da aplicação em uma plataforma onde o processo possa ser automatizado e controlado integralmente, com necessidade mínima de intervenção humana e prontamente adaptável para a maioria dos clientes.

O ARM prima em estabelecer fluxos de processo (chamados de *ARM Workflows*) para garantir que cada requisição de acesso passe por vários estágios processuais antes de o acesso ser atribuído no sistema. Os *ARM Workflows* devem ser criados de modo a satisfazerem os requerimentos da política de acesso do cliente e melhores práticas de mercado – portanto não podem ser simplesmente copiados de um modelo existente.

Apresenta-se a seguir uma possibilidade de *ARM Workflow* para exemplificar os recursos presentes no GRC AC. Assim, para uma solicitação de acesso ao sistema que consiste na adição de novas *Roles* a um usuário existente, pode-se criar o seguinte fluxo:

1. **Preenchimento da requisição de acesso:** para que a requisição de acesso seja iniciada, é necessário que ao menos as seguintes informações sejam fornecidas pelo solicitante:
 - a. Dados pessoais do usuário (nome completo, matrícula, e-mail, *user-ID*);
 - b. Dados organizacionais do usuário (departamento, cargo, gerente);

- c. Justificativa de negócio (um motivo pelo qual o acesso pedido se faz necessário);
- d. *Roles* (ou o acesso sendo requisitado).

Através de diversos conectores externos, o *GRC AC* pode extrair dados automaticamente para o formulário de acesso, excluindo-se a necessidade de preenchimento manual e evitando inconsistências decorrentes do mesmo. Por exemplo: os dados pessoais e organizacionais do usuário podem ser extraídos do Active Directory ou de qualquer outro repositório de identidade presente na empresa.

As *Roles* também podem ser extraídas das instâncias SAP através de conectores. O *GRC AC* pode realizar cargas de dados periódicas entre os sistemas SAP e o *GRC AC*, mantendo o catálogo de *Roles* sempre atualizado. Sgarbi (2013) ressalta que o usuário final por muitas vezes não terá o conhecimento sobre quais *Roles* devem ser requisitadas para se obter os acessos necessários para a sua função. É função do time de Segurança SAP e das linhas de negócio mapear as *roles* a cada função e prover um catálogo de *roles* compreensível e acessível a todos os usuários para evitar que *Roles* sejam requisitadas desnecessariamente.

2. **Aprovações:** uma vez iniciada a solicitação, ela deve ser encaminhada para aprovação dos responsáveis. Recomenda-se que uma solicitação típica a ambiente produtivo contenha os seguintes gestores no fluxo de aprovação:
 - a. Gerente imediato (tendo o gerente acima como substituto);
 - b. Gestor da *Business Role* (cada *role* deve ter seu gestor designado pelo negócio);
 - c. Gestor de Segurança (pode também ser designada ao analista de GRC)

O fluxo de aprovação deve conter gestores competentes para analisar imparcialmente se o acesso sendo requisitado é ou não necessário e se haveriam riscos envolvidos no processo.

3. **Análise de Risco:** logo após as aprovações básicas, a requisição passa por uma análise de risco, na qual se integra parte do componente ARA (*Access Risk Analysis*). A *engine* do ARA é invocada para a execução de um cenário simulado – as *Business Roles* que são parte da requisição são combinadas àquelas já existentes no perfil do usuário para que se gere um relatório que lista todos os conflitos de Segregação de Funções (chamados de *SoD*) e, a partir deles, identificam-se entidades chamadas de *Riscos*. Se *Riscos* forem identificados durante a fase de Análise de Risco, recomenda-se que ações mitigatórias sejam tomadas, e que o fluxo de aprovação se desvie para um novo caminho, de modo a validar, aprovar ou tomar ações mitigatórias contra o risco identificado.

4. **Mitigação de risco:** esse subfluxo só deve ser iniciado caso haja algum *Risco* identificado na fase de Análise de Risco. Nessa fase, recomenda-se que os gestores de segurança e os controladores da área relevante ao risco estudem e decidam se o risco irá coexistir no perfil do usuário, ou se o usuário perderá um dos seus acessos para que o outro seja adicionado. Sendo de natureza situacional, cada caso deve ser analisado e tratado individualmente.

5. **Provisionamento e encerramento da requisição:** após todas as aprovações necessárias, a requisição está pronta para ser atendida. Através dos conectores existentes e o recurso de auto-provisionamento, as *Business Roles* aprovadas são adicionadas ao usuário automaticamente pelo GRC AC, deixando as *Roles* rejeitadas de fora. É possível também automatizar o processo de criação, deleção e *reset* de senha de usuário, utilizando-se dos conectores e *plug-ins* corretos. Notificações automáticas via e-mail também são possíveis de se configurar, fechando o ciclo processual e reduzindo o esforço requerido por requisição de acesso.

Vale frisar que o exemplo apresentado é só um dos *ARM Workflows* que podem ser criados para um tipo de solicitação em específico. Outras espécies de requisição podem ser criadas, com fluxos de processo condizentes às necessidades apresentadas.

7.2 ACCESS RISK ANALYSIS (ARA)

O componente ARA contém um conjunto de ferramentas analíticas dedicadas à detecção preemptiva de *Riscos*. Através de relatórios e integração nativa ao ARM, o ARA protege os sistemas SAP contra conflitos de segregação de função (também chamados de SoD, ou *Segregation of Duties*). Antes de se aprofundar no funcionamento do ARA, é importante que se introduza o conceito de SoD e como este se relaciona à Lei *Sarbanes-Oxley*, popularmente conhecida como SOx.

O ARA (*Access Risk Analysis*) veio em resposta às necessidades introduzidas na seção 404 da Lei SOx. A ferramenta opera em um comportamento análogo a uma Matriz de Funções, que relaciona as ações que resultam em um conflito de *SoD*. Um exemplo básico de Matriz de Funções pode ser visualizado na tabela 1:

Tabela 1: exemplo de *Matriz de Funções*

Roles Function/ Processes	Create Vendor	Change Vendor	Post Goods Receipt	Post Payment	Process Inventory	Goods Issue	Maintain PO
Create Vendor		X	X	X			X
Change Vendor	X		X	X			X
Post Goods Receipt	X	X		X	X	X	X
Post Payment	X	X	X			X	X
Process Inventory			X				X
Goods Issue			X	X			
Maintain PO	X	X	X	X	X		

X - Existence of Conflict

Fonte: Khan, 2007, p. 4.

O exemplo, embora minimalista, ilustra bem o funcionamento de uma Matriz de Funções e como ela identifica potenciais conflitos de SoD. Uma vez que um usuário possua os acessos marcados como conflitantes – tal como a habilidade de criar um

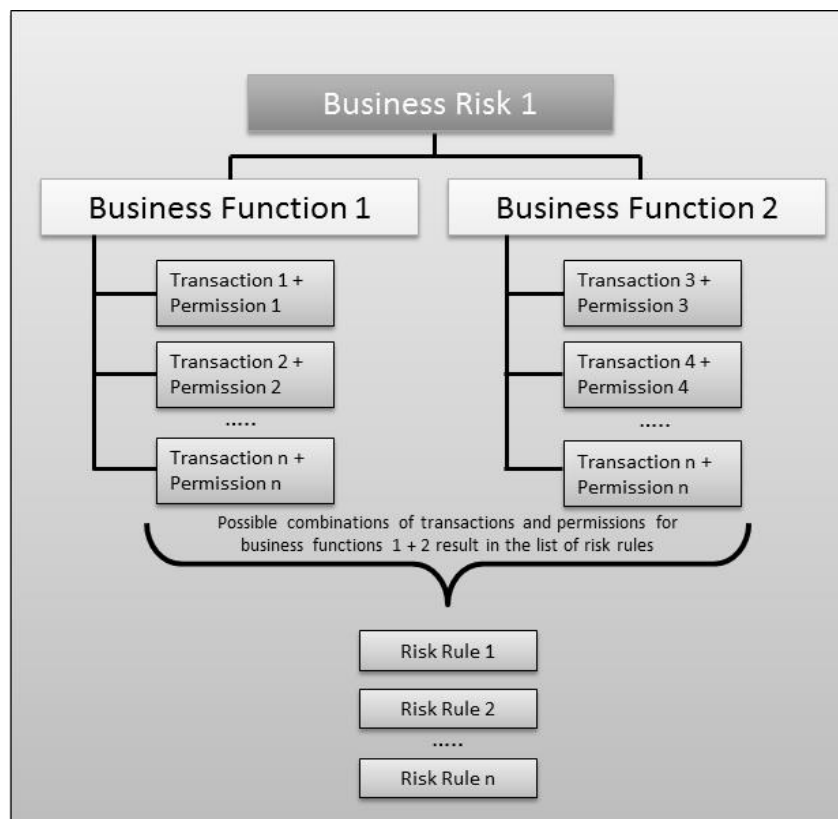
fornecedor e postar pagamentos – o sistema irá identificar essa ação como um conflito de SoD, e gerar um *Risco* a partir deste.

Entretanto, na prática, os conflitos de SoD não serão simplistas como ilustrados na tabela 1, dada a natureza complexa dos acessos no sistema SAP e as várias funções presentes num sistema ERP integrado tal como o SAP. Um dos conceitos introduzidos existentes no contexto SAP é o de conflitos a nível de *Ações (Action Level)* e *Permissões (Permission Level)*:

- *Action Level*: refere-s aos conflitos encontrados no nível de Transação (ou *T-code*), levando-se em conta somente o propósito geral da mesma.
- *Permission Level*: considera conflitos entre os objetos de autorização (*Authorization Objects*), que por sua vez podem estar ligados a multiplas T-codes.

Ações e *Permissões* compõem a estrutura mais básica da entidade conhecida no GRC como *Risco* ou *Risk*.

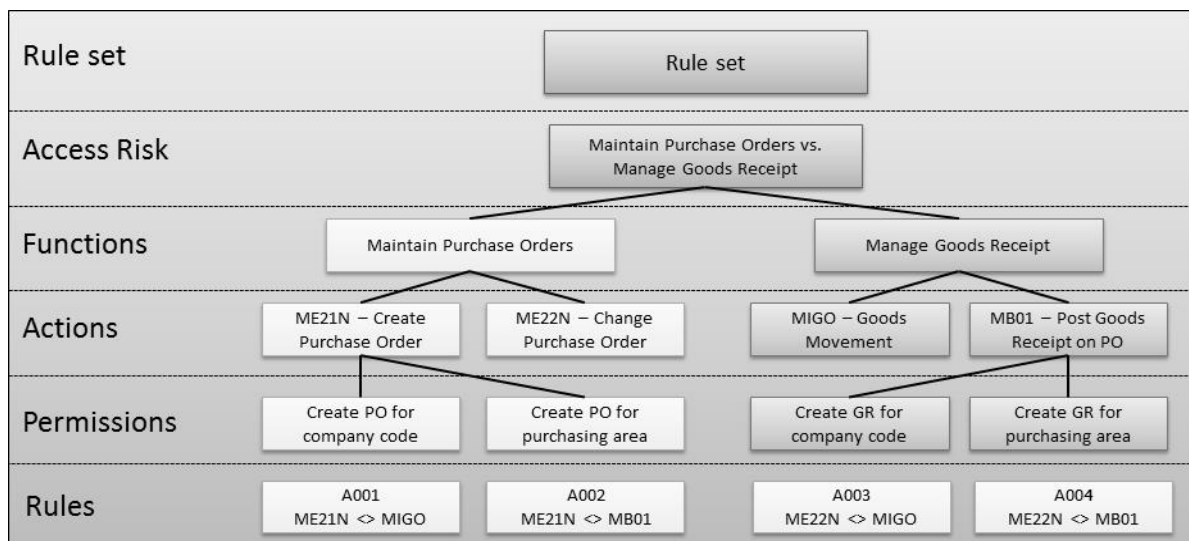
Figura 13 – Funções como parte de um *Risco*



Fonte: Banzer, 2014

Alessandro Banzer (2014) define o Risco no GRC como composto por ao menos duas Funções conflitantes. As Funções, por sua vez, são formadas por conjuntos de Ações (T-codes) ou Permissões (Objetos de Autorização). As possíveis combinações entre Ações e Permissões entre as duas ou mais funções resultam numa entidade conhecida como *Regra* ou *Risk Rules*. Estas se fazem necessárias, pois existem Ações ou T-codes diferentes que convergem num mesmo propósito—porém com nuances diferenciadas. As *Regras* auxiliam o GRC ARA a agrupar as Ações para que as *Funções* permaneçam consistentes. O conjunto de Regras, Funções e Riscos é chamado de *Rule Set* ou Matriz de Risco, conforme mencionado anteriormente. A figura 14 mostra um exemplo relacionando todas as entidades:

Figura 14 – Regras, Funções e Riscos como parte do Rule Set



Fonte: Banzer, 2014

O ARA já possui, por padrão, um *Rule Set* chamado de *Rule Set Global*. Essa matriz contém todas as regras e riscos possíveis e existentes na maioria dos negócios. Desta forma, deve-se criar uma *Rule Set* customizada, tendo a *Rule Set* padrão como base e eliminando-se as regras que não estão em escopo para o cliente atual. Note-se que mesmo a *Rule Set* padrão não inclui riscos gerados por programas customizados (programas ABAP iniciados em Z ou Y). As regras para programas customizados devem ser criadas manualmente na *Rule Set* do cliente.

Tendo-se em vista esta complexidade na definição dos *Riscos*, é necessário que se implemente o ARA com uma abordagem sistêmica, na qual a própria SAP recomenda um processo de seis passos, baseado em melhores práticas de mercado.

1. Reconhecimento dos *Riscos*
 - 1.1. Identificar *Riscos*
 - 1.2. Aprovar exceções
 - 1.3. Categorizar riscos como *Baixo, Médio* ou *Alto*
2. Construção e validação de *Regras*
 - 2.1. Utilizar melhores práticas de mercado para criação do conjunto de *Regras*
 - 2.2. Validar, customizar e testar *Regras*
 - 2.3. Contextualizar regras em nível de usuários e *Roles*
3. Análise de Risco
 - 3.1. Rodar relatórios de Análise de *Risco*
 - 3.2. Estimar esforços de remediação
 - 3.3. Analisar *Roles* e usuários
 - 3.4. Modificar *Regras* baseado em análise, se necessário
 - 3.5. Caso necessário, configurar mecanismos de alerta para *Riscos* que se concretizarem
4. Remediação
 - 4.1. Determinar alternativas para eliminação de *Riscos*
 - 4.2. Utilizar dados da Análise para nortear ações corretivas
 - 4.3. Documentar aprovações para ações corretivas
 - 4.4. Modificar *Roles* ou usuários
5. Mitigação
 - 5.1. Determinar controles alternativos para riscos que não podem ser remediados
 - 5.2. Educar os gestores sobre as aprovações de *Risco* e ações de monitoramento
 - 5.3. Criar e documentar um processo para monitoramento de *Risco*
 - 5.4. Implementar mecanismos de monitoramento (controles)
6. Conformidade contínua
 - 6.1. Comunicar mudanças que serão feitas a *Roles* ou usuários
 - 6.2. Simular mudanças a *Roles* ou usuários
 - 6.3. Implementar alertas nos controles de monitoramento quando possível
 - 6.4. Testar controles de mitigação

O próprio fabricante também lista uma matriz de papéis e responsabilidades. Esta matriz pode ser encontrada no Anexo A.

7.3 BUSINESS ROLE MANAGEMENT (BRM)

Nativamente, o SAP não oferece uma solução para integrar o gerenciamento de *Roles* em um ambiente SAP heterogêneo. Por consequência, a gestão descentralizada pode vir a gerar dificuldades e altos custos com a equipe de segurança para manter as operações.

A solução oferecida pelo BRM (*Business Role Management*) inclui um modelo centralizado de gestão de *Roles*, assim como opções na metodologia utilizada e integração com o componente ARA, assegurando uma gestão mais limpa, simplificada e livre de SoDs para empresas com múltiplas instâncias SAP.

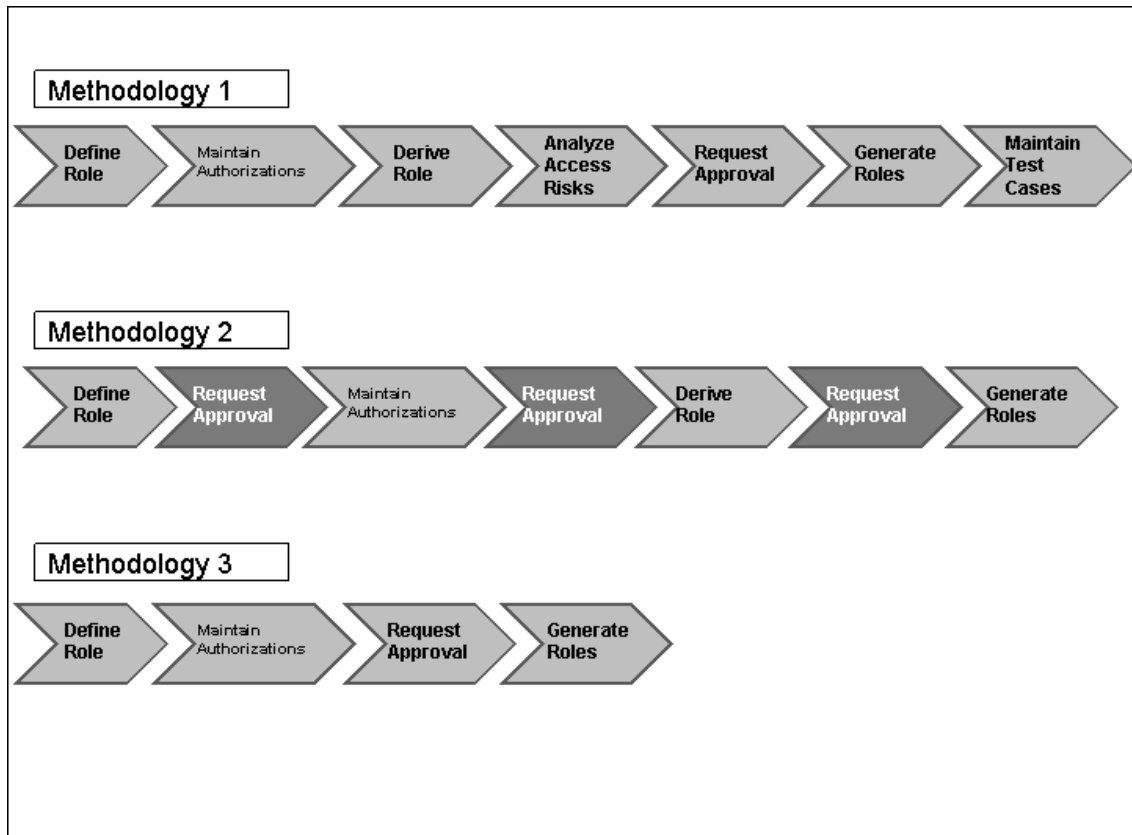
O fabricante afirma que, através de conexões RFC feitas através de conectores integrados, o GRC busca dados das múltiplas instâncias SAP e as converge dentro do GRC, transformando o mesmo em sua única plataforma gestão.

Entre as funcionalidades do BRM, pode-se destacar:

- Criação de fluxos de processo específicos para criação ou manutenção de *Role*;
- Possibilidade de se acompanhar o progresso de criação ou alteração da *Role*;
- Realização de análise de risco em tempo de manutenção;
- *Logs* de modificações disponíveis para todas as ações realizadas em *Roles*;
- Múltiplas metodologias disponíveis para cada tipo de *Role*.

Dependendo das políticas e processos de manutenção de *Roles*, o GRC oferece vários fluxos de processo, chamados de *Metodologia de Manutenção*. A figura 15 ilustra alguns exemplos de Metodologias para o BRM:

Figura 15 – Exemplos de Metodologias de Manutenção



Fonte: SAP SE [ca. 2013]

Pode-se optar por uma Metodologia mais completa, como ilustrada no exemplo número 1, em que todos os passos típicos da manutenção de *Role* são incluídos da seguinte maneira:

1. *Define Role*: neste passo cria-se os atributos mais básicos que definem a role, tais como:
 - 1.1. Nome (podendo ou não possuir máscaras de nomenclatura)
 - 1.2. Tipo de Role
 - 1.3. Sensibilidade/Criticalidade
 - 1.4. Companhia
 - 1.5. Área Funcional
 - 1.6. Pré-requisitos (caso necessário previamente para atribuição a usuários)
 - 1.7. Processo de Negócio
 - 1.8. Subprocesso de Negócio
 - 1.9. Outros campos customizáveis

2. *Maintain Authorizations*: aqui entram os dados técnicos de autorização da *Role*. Usualmente feito pelo time de Segurança, envolve a tradução de requisitos de negócio em campos técnicos nos Objetos de Autorização.
3. *Derive Role*: caso a *Role* deva possuir versões derivadas (como, por exemplo, uma segunda versão da mesma *role* voltada para funcionários de outra localização geográfica ou outra companhia), esta tarefa pode ser automatizada através dos recursos providos neste passo.
4. *Analyze Access Risks*: através da integração com o ARA, o sistema checa a *Role* por possíveis conflitos de SoD e alerta o desenvolvedor na presença de algum Risco.
5. *Request Approval*: o sistema pode ser configurado para automaticamente buscar aprovação do Gestor da *Role* ou de qualquer outro indivíduo incumbido das aprovações para aquela dada *Role*.
6. *Generate Roles*: uma vez aprovada, a *Role* passa a ser validada e ativada dentro do sistema SAP escolhido.
7. *Maintain Test Cases*: neste passo realizam-se e documentam-se as atividades de teste funcional e técnico da *Role* em questão.

Fluxos mais simples ou mais complexos podem ser implementados utilizando os recursos supracitados, de acordo com as necessidades do negócio.

Sem o GRC EAM, em cenários em que o usuário necessita de acessos excepcionais em caráter emergencial num sistema SAP, os administradores de usuário e equipe de segurança eram responsáveis por prover acesso temporário a uma conta de usuário ou *Role* com alto privilégio. No entanto, não havia garantia em relação ao abuso da tal *Role* ou conta. Uma vez que os logs demoravam dias para serem gerados, a possibilidade de uma fraude se concretizar e passar despercebida nestes cenários era alta.

Além de *logs* de registro em tempo real, o GRC EAM também oferece um conjunto de ferramentas que facilitam a gestão dos usuários de emergência, provendo controle e visibilidade das atividades que ocorrem nestes cenários.

Utilizando-se da integração com o ARM, o fluxo de aprovação necessário para a obtenção de um acesso emergencial pode ser criado e automatizado completamente, de forma a estabelecer um prazo de acesso (de 8 a 48 horas, por exemplo) e a obter pré-aprovações de todos os gestores envolvidos. Donos de ID Firefighter (chamados de *Firefighter Owners*) e controladores dedicados (*Controllers*) também podem ser nomeados e de modo a fazer parte do fluxo de aprovação ou de tarefas de manutenção de um designado *Firefighter ID*.

. A ferramenta pode operar sob duas estratégias distintas: a de Usuário de Emergência (*Firefighter ID*) ou via *Role* de Emergência (*Firefighter Role*).

- EAM baseado em *Firefighter ID*: é criada uma conta de usuário que contém Roles de alto privilégio. Pode-se criar quantos IDs forem necessários e também segmentá-los por área de negócio, propósito ou localidade – dado que as suas *Roles* sejam desenhadas especificamente para este propósito. Uma vez obtidas todas as aprovações necessárias para sua obtenção e designado o seu tempo de uso, o usuário pode utilizar o *Firefighter ID* através de uma troca de sessão via RFC – que consiste em logar no sistema central do GRC EAM, acessar a *T-code* central de gerenciamento do EAM e clicar no botão “Logon” que estará disponível para o *Firefighter ID*. A partir deste ponto, o usuário deixa a sua própria sessão e passa a logar-se como o próprio *Firefighter ID*, assumindo seus acessos e privilégios. Inicia-se também um rastreamento ativo de todas as atividades que o usuário realiza enquanto logado como o *Firefighter ID*. Os administradores e gestores podem receber todos os *logs* via e-mail em tempo real, incluindo data e hora do *login*, *T-codes* acessadas, e até mesmo

visualizar os registros inseridos, modificados ou apagados do banco de dados. No caso de fraude ou mau-uso do Firefighter ID, os gestores e administradores podem ser notificados via alerta de e-mail e tomar as ações necessárias em tempo hábil. Uma vez expirado o prazo de uso, os *logs* podem também ser automaticamente enviados para revisão e aprovação dos gestores da área, provendo assim uma rede extra de proteção contra fraudes ou abuso dos privilégios do *Firefighter ID*.

- EAM baseado em *Firefighter Role*: parte dos mesmos princípios que o modelo baseado em Firefighter ID, porém consiste em assinalar uma Role (que seria tipicamente atrelada ao Firefighter ID no modelo anterior) ao próprio usuário. Este modelo é pouco utilizado pela dificuldade encontrada na geração dos *logs*, uma vez que o sistema é, por padrão, configurado para ativar *logs* em usuários *Firefighter ID*, não em usuários comuns.

Tendo-se ambos os cenários em vista, cabe ao negócio e à equipe de segurança estimar a melhor solução e aplicá-la de modo a cobrir as necessidades e prover pleno controle sobre a gestão dos usuários de emergência via EAM.

Sabendo-se dos recursos oferecidos pelo *GRC Access Control*, é de interesse do autor descobrir se esta realmente satisfaz as necessidades encontradas pelos clientes em seus locais de trabalho.

8 ESTUDO DE MERCADO

Tendo em vista o potencial da ferramenta, criou-se um estudo de mercado para avaliar o nível de satisfação dos clientes e/ou prestadores de serviços em relação ao pacote de aplicações *GRC Access Control*.

Um questionário público foi criado através da ferramenta *SurveyMonkey* (www.surveymonkey.com) e divulgado em grupos voltados à segurança SAP e/ou gerência de projetos, dentro da rede social profissional *LinkedIn*. Divulgação informal também foi feita, tendo como alvo clientes no qual o autor já prestou serviço em seu ambiente de trabalho.

O questionário de respostas fechadas consiste em seis questões que têm por objetivo medir o grau de efetividade do GRC, o grau de satisfação do público-alvo e a atribuição de fatores que levariam a ferramenta a obter um melhor desempenho em seu ambiente de trabalho.

O questionário está disponível, em português e inglês, via Anexo B.

9 ANÁLISE DE RESULTADOS

Após a coleta de respostas, o resultado foi contabilizado pela ferramenta SurveyMonkey. Os dados foram coletados após 14 respostas, no dia 10 de novembro de 2014. Os resultados por questão são apresentados a seguir e podem ser visualizados graficamente via Anexo C:

1. *Governança, Conformidade e Gestão de Risco são prioridades na sua empresa?*
 - a. Sim (85,71% ou 12 respostas)
 - b. Não (14,29% ou 2 respostas)

Corroborando a ideia apresentada na pesquisa realizada pela *McKinsey & Co.* no capítulo 6, a grande maioria dos clientes tem a metodologia do GRC (Governança, Risco e Conformidade) como prioridade em seus negócios – sugerindo que um bom desempenho do SAP GRC é exigido.

2. *Desde a implementação do GRC, existiram casos confirmados de falha de auditoria ou fraude financeira?*
 - a. Sim (14,29% ou 2 respostas)
 - b. Não (42,86% ou 6 respostas)
 - c. Não sei responder (42,86% ou 6 respostas)

Apesar de muitos dos entrevistados não saberem ou optarem por não responder, grande parte dos clientes não sofreu com penalidades causadas por falhas de auditoria. Dentro do conjunto universo dos oito indivíduos que souberam responder a essa questão, 75% afirmam não ter experimentado falhas ou fraudes, enquanto 25% alegam o contrário. Mesmo dado o pequeno número do conjunto, a porcentagem de entrevistados que afirma ter sido afetados por fraude ou falhas de auditoria sugere que o SAP GRC não é infalível, e que existem motivos para que tais desvios aconteçam.

3. *"A ferramenta GRC é indispensável para a gestão segura de meus sistemas SAP."*

- a. Concordo plenamente (28,57% ou 4 respostas)
- b. Concordo (57,14% ou 8 respostas)
- c. Discordo (14,29% ou 2 respostas)
- d. Discordo plenamente (0% ou 0 respostas)

Esta questão visa determinar se há, entre os entrevistados, a propensão de substituir a ferramenta SAP GRC por alguma outra solução do mercado. Os resultados apresentam uma tendência positiva ao SAP GRC e uma fraca ocorrência de insatisfação.

4. *"A gestão dos meus sistemas SAP via GRC me auxilia a manter os Riscos financeiros sob controle."*
- a. Concordo plenamente (28,57% ou 4 respostas)
 - b. Concordo (71,43% ou 10 respostas)
 - c. Discordo (0% ou 0 respostas)
 - d. Discordo plenamente (0% ou 0 respostas)

Pode ser visualizada através desta questão a parcela pela qual a ferramenta SAP GRC é responsável pela gestão e controle dos riscos financeiros dentro das companhias. Resultados positivos sugerem que a empresa é dependente da ferramenta para a tarefa de gestão de risco, ao passo que respostas negativas sugerem que a ferramenta é dispensável para esta tarefa, presumindo-se que a companhia disponha de outros métodos para o controle dos riscos. Neste caso, observa-se que não há ocorrência de respostas negativas em ambos os espectros.

5. *"Os recursos do GRC poderiam ser mais bem aproveitados se minhas equipes (técnica, gestores, usuários finais) tivessem melhor treinamento e capacitação."*

- a. Concordo plenamente (57,14% ou 8 respostas)
- b. Concordo (35,71% ou 5 respostas)
- c. Discordo (0% ou 0 respostas)
- d. Discordo plenamente (7,14% ou 1 resposta)

Numa tentativa de identificar pontos de melhoria, a questão n° 5 aponta as equipes que configuram ou utilizam o GRC como um dos possíveis elos fracos da cadeia de processo, questiona o entrevistado acerca da possibilidade de melhoria do desempenho do sistema caso seu capital humano fosse mais bem-preparado ou treinado para a utilização do SAP GRC. Observa-se uma forte tendência positiva e uma tímida ocorrência negativa em forma de uma resposta à alternativa d; o que nos leva a concluir que treinamento e capacitação são um dos desafios encontrados na gestão de sistemas via SAP GRC.

6. De maneira geral, o quão satisfeito você está com relação ao desempenho do GRC na sua empresa?

- a. Muito satisfeito (21,43% ou 3 respostas)
- b. Insatisfeito (35,71% ou 5 respostas)
- c. Nem satisfeito, nem insatisfeito (28,57% ou 4 respostas)
- d. Insatisfeito (14,29% ou 2 respostas)
- e. Muito insatisfeito (0% ou 0 respostas)

Com caráter generalista, a questão final avalia o quão satisfeitos os entrevistados estão com a solução GRC existente na empresa, e não em relação à ferramenta em si. Observa-se que maioria dos entrevistados está de fato satisfeita, enquanto uma parcela menor opta pela neutralidade e uma parcela ainda menor demonstra insatisfação em relação à performance do produto.

10 CONSIDERAÇÕES FINAIS

A partir dos resultados obtidos no questionário, restrito à pequena escala das companhias entrevistadas, pode-se afirmar que:

1. GRC continua sendo prioridade de investimento em grande parte das empresas;
2. A ferramenta SAP GRC pode vir, em alguns casos, a não atender as necessidades do negócio;
3. O mercado não tende a substituir o SAP GRC por alguma outra ferramenta similar;
4. Grande parte das companhias que utilizam SAP dependem exclusivamente do SAP GRC para a gestão de seus riscos financeiros;
5. Treinamento e capacitação contínua são um desafio para grande parte das empresas;
6. Uma moderada parcela do mercado está satisfeita com o SAP GRC, mas está à espera de melhoria em algumas áreas.

À luz destas conclusões, retrata-se um mercado fidelizado e relativamente satisfeito com a performance da sua solução SAP GRC, mas que ainda espera por melhorias; tendo-se a questão do treinamento e capacitação como um dos exemplos. É compreensível que muitos dos profissionais de segurança no ramo do SAP GRC não tenham pleno conhecimento técnico devido a certas dificuldades encontradas no mercado de treinamento. Atualmente, os cursos oficiais para SAP GRC são encontrados a valores que superam R\$ 10.000,00 – o que inibe o ingresso de muitos novos profissionais na área. Uma boa iniciativa na área se dá em forma de parcerias entre a SAP e as consultorias, que recebem créditos para treinamento em troca de serviços ou vendas, acordados em contrato.

Vale frisar que o SAP GRC e seus treinamentos são uma das linhas de negócio da própria SAP SE, tendo como um dos objetivos a movimentação de capital e geração de lucros. Portanto, neste cenário, é seguro afirmar que muitos profissionais independentes da área de segurança tenham que lidar com as crescentes expectativas do mercado e os interesses financeiros do fabricante ao mesmo tempo;

o que pode resultar num ingresso no mercado de trabalho sem os devidos treinamentos e certificações.

Além da questão do treinamento, também se pode levantar uma questão em relação aos motivos responsáveis pela insatisfação ou até mesmo pelas falhas de auditoria ou fraudes, conforme mencionados na pergunta n° 5 do questionário. Se gerados pelo próprio cliente, requer-se uma pesquisa acerca dos motivos que levam a implementação do GRC a ser inefetiva e como resolvê-los. Se dadas por limitações da própria ferramenta, sugerir ao fabricante ideias prototipadas de como melhorar as funcionalidades deficitárias.

Em relação à fidelização, pode-se atribuir a grande aderência dos clientes ao SAP GRC por simplesmente se tratar do que atualmente é a solução mais aceita de mercado para a gestão de sistemas SAP. Uma vez que o pacote é desenvolvido pela própria SAP SE, não é comum que se haja concorrência.

Entretanto, somente esta pesquisa não é suficiente para se determinar as áreas críticas de melhoria e as principais necessidades do mercado. Com esta, abre-se o caminho para que posteriores trabalhos aprofundem-se nas questões aqui apresentadas e possam contribuir ao mercado, gerando sistemas de informação mais robustos e seguros, e à área acadêmica, ampliando os patamares da metodologia GRC e conseqüentemente da segurança de sistemas de informação.

REFERÊNCIAS BIBLIOGRÁFICAS

- ALECRIM, E. **O que é ERP (Enterprise Resource Planning)?** Blog Info Wester. Junho de 2010. Disponível em: <http://www.infowester.com/erp.php>. Data de acesso: 1 de setembro de 2014
- BANZER, A. **Business Risks/Rule Set.** SAP Community Network. Abril de 2014. Disponível em: <http://scn.sap.com/docs/DOC-54434>. Data de acesso: 20 de Outubro de 2014.
- BODDU, R. **GRC Access Control 10 – What’s new?** SAP Security Expert. Agosto de 2011. <http://www.sapsecurityexpert.com/2011/08/grc-access-control-10-whats-new/>. Data de acesso: 27 de Outubro de 2014.
- BRATTON, W. **Enron and the Dark Side of Shareholder Value.** Washington, DC: The George Washington University Law School, 2002. 79 p.
- BROADY, D. V.; ROLAND, H. A. **SAP GRC for Dummies.** Hoboken, NJ: John Wiley & Sons, 2008. 342 p.
- COLUMBUS, L. **2013 ERP Market Share Update: SAP Solidifies Market Leadership.** Forbes. Dezembro de 2013. Disponível em: <http://www.forbes.com/sites/louiscolombus/2013/05/12/2013-erp-market-share-update-sap-solidifies-market-leadership/>. Data de acesso: 17 de outubro de 2014.
- DE BRUYN, G.M.; LYFAREFF, R.W. **Introduction to ABAP/4 Programming for SAP.** Portland, OR: Premier Press. 1998. 440p.
- HIRAO, J. et al **SAP Security Configuration and Deployment: The IT Administrator's Guide to Best Practices.** Boston, MA: Syngress Publishing, 2009. 391 p.

KHAN, N. **Segregation of Duties – SoD**. SAP Developer Network. Outubro de 2007.

Disponível em:

<http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/f02855c9-2091-2a10-8682-af41abe087ba?overridelayout=true> Data de acesso: 29 de Outubro de 2014

LABADESSA, E; BITTENCOURT, M; ROBERTO, M; ROSSINI, A. **O SAP e a Governança de TI: suas contribuições para as melhores práticas nas organizações**. Volume 1, número 1 – 2011. Disponível em:

<http://revistaseletronicas.fmu.br/index.php/rms/article/view/51/pdf>. Data de acesso: 11 de setembro de 2014.

PricewaterhouseCoopers. **The Global State of Information Security® Survey 2015**. Disponível em: <http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml#>. Data de acesso: 13 de outubro de 2014.

SAP SE. **Role Creation Methodology**. SAP Help Library. [ca. 2013] Disponível em: http://help.sap.com/saphelp_grcac101/helpdata/en/3a/e3e44fc5c54a59e10000000a445394/content.htm?frameset=/en/2a/39243029c441d2a6c4a56a4a91ba49/frameset.htm¤t_toc=/en/8b/dd50b2b1f34e049c45ded84788789c/plain.htm&node_id=128&show_children=false. Data de acesso: 17 de Outubro de 2014.

SGARBI, L. F. **SAP Access Control 10.0 - Implementation and Configuration**. GRC 300. SAP Training Center. Avenida Paulista, 2073 - Edifício Horsa II, São Paulo. 22 a 26 de julho de 2013. Curso presencial.

SGARBI, L. F. **SAP Governance, Risk, and Compliance (GRC) 10.0 Principles and Harmonization**. GRC 100. SAP Training Center. Avenida Paulista, 2073 - Edifício Horsa II, São Paulo. 4 a 5 de julho de 2013. Curso presencial.

SHAUL, L.; TAUBER, D. **Critical Success Factors in Enterprise Resource Planning Systems: Review of the Last Decade**. ACM Computing Surveys, vol. 45. 2013. 35 p.

SOLUTIONS, K. G. **SAP ABAP Questions and Answers**. Sudbury, MA: Jones and Bartlett Publishers, 2010. 250p.

TORCK, C. **Por que ter um ERP?** PartnerSales. São Paulo, SP. Outubro de 2011. Disponível em: <http://www.partnersales.com.br/artigo/501/por-que-ter-um-erp>. Data de acesso: 17 de setembro de 2014.

VAN DROOGENBROEK, I.; RYMEN, W.; WAUTERS, K. **Governance, risk & compliance technology for organisations running SAP: Trends, analysis & insights on the Belgian market**. PricewaterhouseCoopers. 2013. Disponível em: <http://www.pwc.be/en/publications/2013/grc-survey-belgium.pdf>. Data de acesso: 18 de outubro de 2014.

VAN HOLSBECK, M. **Security in an ERP World**. Help Net Security. Maio de 2004. Disponível em: <http://www.net-security.org/article.php?id=691>. Data de acesso: 17 de setembro de 2013.

VOGEL, A; KIMBELL, I. **MySAP ERP for Dummies**. Hoboken, NJ: John Wiley & Sons, 2008. 314 p.

WAILGUM, T. **The Biggest Loser in Oracle-Sun Deal: SAP**. CIO. Framingham, MA. Abril de 2009. Disponível em: <http://www.cio.com/article/2373379/enterprise-software/the-biggest-loser-in-oracle-sun-deal--sap.html>. Data de acesso: 13 de Julho de 2014.

ANEXO A – MATRIZ DE PAPÉIS E RESPONSABILIDADES DO ARA

Papel	Responsabilidade
Dono de Processo de Negócio	<ul style="list-style-type: none"> • Identificar/aprovar Riscos para posterior monitoramento; • Aprovar ações de remediação para acessos de usuário; • Desenhar controles para conflitos de mitigação; • Comunicar mudanças feitas à distribuição ou composição das <i>Business Roles</i>; • Realizar atividades de conformidade contínua proativamente.
Executivos e Gerentes Sênior	<ul style="list-style-type: none"> • Aprovar ou rejeitar riscos que envolvam múltiplas áreas de negócio; • Aprovar <i>Controles de Mitigação</i> para cobertura de <i>Riscos</i>.
Analista de Segurança	<ul style="list-style-type: none"> • Responsáveis pela arquitetura técnica do GRC e seus processos; • Criar e gerir <i>Regras</i> para identificação de riscos de negócio; • Customizar a arquitetura técnica do GRC para que as políticas de segregação de funções sejam cumpridas; • Analisar e remediar conflitos de SoD em nível de <i>Role</i>.
Auditor interno	<ul style="list-style-type: none"> • Realizar as avaliações de risco regularmente; • Prover especificações e requisitos para posterior auditoria; • Realizar testes periódicos das <i>Regras</i> e <i>Controles de Mitigação</i>; • Agir como ponto de contato para auditores externos.

Gestor de Regras	<ul style="list-style-type: none">• Não pode ser envolvido em quaisquer tarefas inerentes ao grupo dos Analistas de Segurança;• Responsável pela integridade e controle das <i>Regras</i> e do <i>Rule Set</i>;• Pode agir como ponto de contato entre a equipe de <i>Basis</i> e equipe técnica do GRC.
------------------	--

ANEXO B – QUESTIONÁRIO

Português:

1. Governança, Conformidade e Gestão de Risco são prioridades na sua empresa?

- Sim
- Não

2. Desde a implementação do GRC, houveram casos confirmados de falha de auditoria ou fraude financeira?

- Sim
- Não
- Não sei responder

3. "A ferramenta GRC é indispensável para a gestão segura de meus sistemas SAP."

- Concordo plenamente
- Concordo
- Discordo
- Discordo plenamente

4. "A gestão dos meus sistemas SAP via GRC me auxilia a manter os Riscos financeiros sob controle."

- Concordo plenamente
- Concordo
- Discordo
- Discordo plenamente

5. "Os recursos do GRC poderiam ser melhor aproveitados se minhas equipes (técnica, gestores, usuários finais) tivessem melhor treinamento e capacitação."

- Concordo plenamente
- Concordo
- Discordo
- Discordo plenamente

6. De maneira geral, o quão satisfeito você está com relação ao desempenho do GRC na sua empresa?

- Muito satisfeito
- Satisfeito
- Nem satisfeito, nem insatisfeito
- Insatisfeito
- Muito insatisfeito

Inglês:

1. Is GRC (Governance, Compliance and Risk Management) a priority for your company?

- Yes
- No

2. Since SAP GRC was implemented, was there any occurrence of fraud or audit failure?

- Yes
- No
- I don't know

3. "SAP GRC is a key tool for the management of my SAP systems."

- Strongly agree
- Agree
- Disagree
- Strongly disagree

4. "Managing SAP systems through GRC helps me keep financial risks under control."

- Strongly agree
- Agree
- Disagree
- Strongly disagree

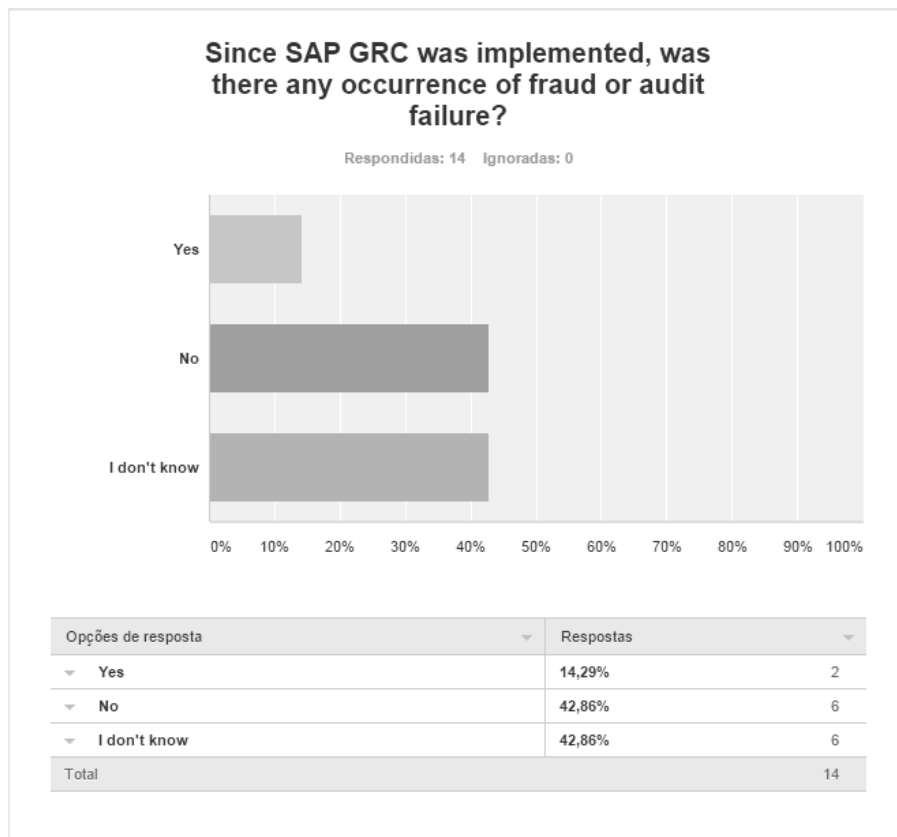
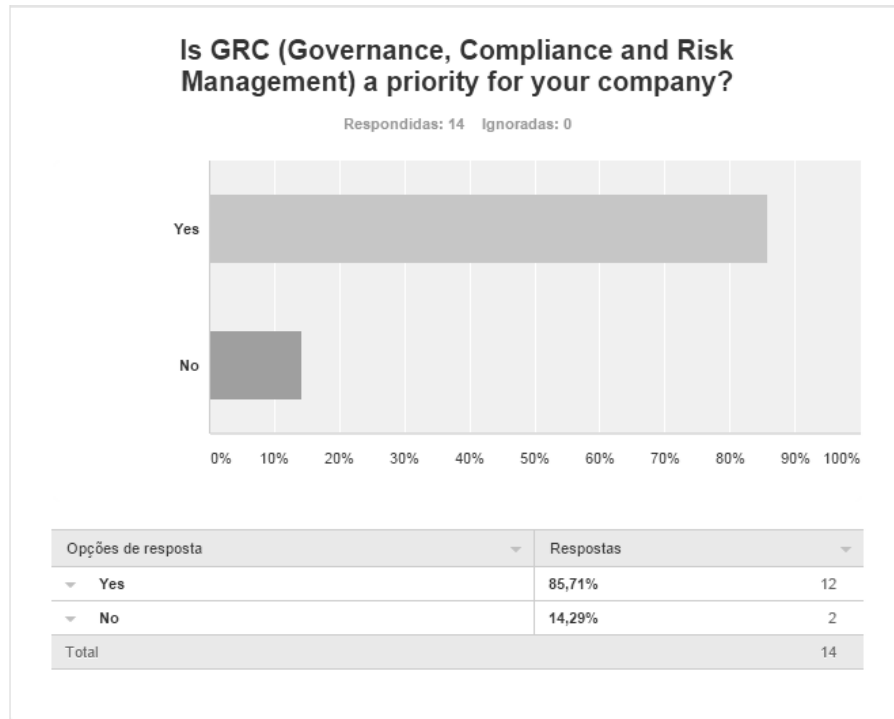
5. "The GRC resources I own could be better used if my teams (tech support, business, end users) had better training and engagement."

- Strongly agree
- Agree
- Disagree
- Strongly disagree

6. How overall satisfied are you with the performance of the GRC suite in your company?

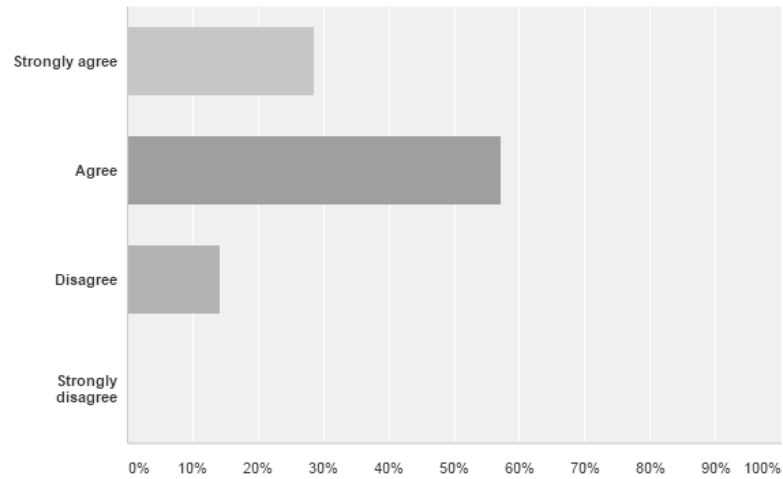
- Very satisfied
- Satisfied
- Neither satisfied nor unsatisfied
- Unsatisfied
- Very unsatisfied

ANEXO C – GRÁFICOS DE RESULTADOS DO QUESTIONÁRIO



"SAP GRC is a key tool for the management of my SAP systems."

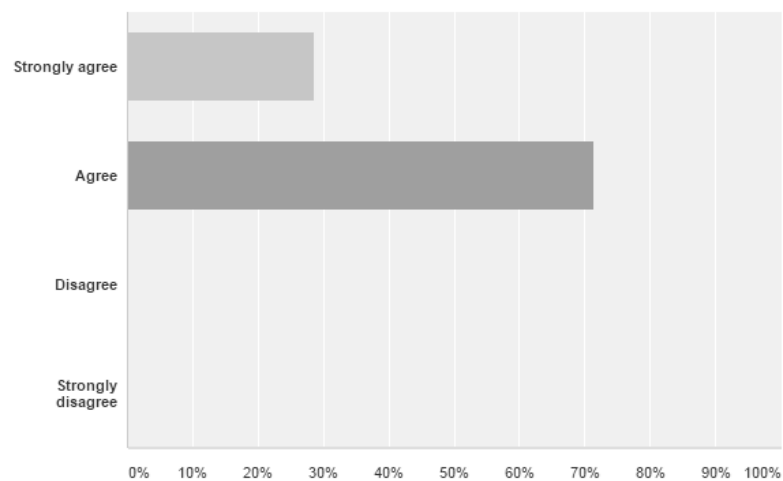
Respondidas: 14 Ignoradas: 0



Opções de resposta	Respostas
Strongly agree	28,57% 4
Agree	57,14% 8
Disagree	14,29% 2
Strongly disagree	0,00% 0
Total	14

"Managing SAP systems through GRC helps me keep financial risks under control."

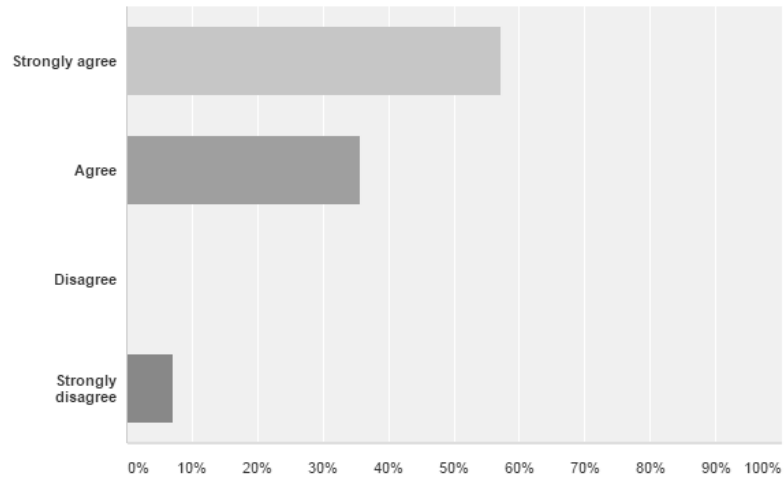
Respondidas: 14 Ignoradas: 0



Opções de resposta	Respostas
Strongly agree	28,57% 4
Agree	71,43% 10
Disagree	0,00% 0
Strongly disagree	0,00% 0
Total	14

"The GRC resources I own could be better used if my teams (tech support, business, end users) had better training and engagement."

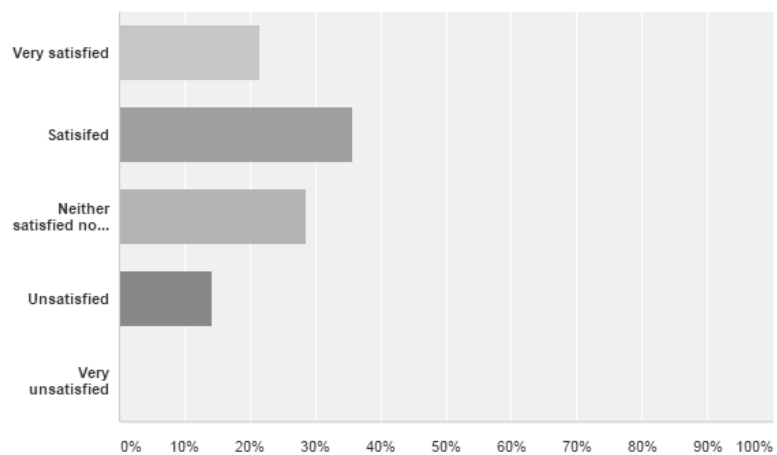
Respostas: 14 Ignoradas: 0



Opções de resposta	Respostas
Strongly agree	57,14% 8
Agree	35,71% 5
Disagree	0,00% 0
Strongly disagree	7,14% 1
Total	14

How overall satisfied are you with the performance of the GRC suite in your company?

Respostas: 14 Ignoradas: 0



Opções de resposta	Respostas
Very satisfied	21,43% 3
Satisfied	35,71% 5
Neither satisfied nor unsatisfied	28,57% 4
Unsatisfied	14,29% 2
Very unsatisfied	0,00% 0
Total	14

ANEXO D – GLOSSÁRIO

Termo	Definição
<i>Action</i> (Ação)	No âmbito do GRC, se refere a uma Transação (ou T-code) dentro do sistema SAP.
<i>Authorization</i> (Autorização)	Pode ser formado por um ou mais Objetos de Autorização e provê acesso a uma determinada parte do sistema SAP.
<i>Authorization Field</i> (Campo de Autorização)	Constitui o nível mínimo da estrutura de autorização do sistema SAP. Pode estar ligado a uma entidade de banco de dados ou outros elementos que façam parte do conjunto de informações que se queira proteger.
<i>Authorization Object</i> (Objeto de Autorização)	Formado pelo conjunto de Campos de Autorização.
<i>Authorization Profile</i> (Perfil de Autorização)	Formado por um conjunto de autorizações, tipicamente construída para proporcionar acesso suficiente para um dado cargo ou ocupação.
Basis	Refere-se ao módulo técnico do sistema SAP. Compreende todas as atividades relacionadas à instalação, configuração, banco de dados e infraestrutura típicas de um sistema SAP.
Conflitos de SoD	Do inglês <i>Segregation of Duties</i> , refere-se a conflitos que surgem caso a devida segregação de funções não seja aplicada em processos de risco de uma empresa.
CRM	Do inglês <i>Customer Relationship Management</i> , define os softwares voltados à gestão de relacionamento com o cliente.
ECC	<i>Enterprise Central Component</i> , ou o produto principal do sistema SAP ERP.
Função	É formado por duas ou mais Ações ou Permissões, de modo a formar as autorizações inerentes a um dado processo de negócio.
GRC	Do inglês <i>Governance, Risk and Compliance</i> (Governança, Risco e Conformidade), é um termo utilizado para descrever a metodologia que converge as áreas de Governança, Gestão de Risco e Conformidade em um único modelo gerenciável.
Permissão	No âmbito do GRC, refere-se a um Objeto de Autorização dentro do sistema SAP.
Risco	Atividade que, se atribuída ao mesmo indivíduo, apresenta perigo à integridade do negócio. É tecnicamente formado por duas ou mais Funções.
<i>Risk Rule</i> (Regra de Risco)	Determina as relações entre ações e permissões, auxiliando o sistema a identificar conflitos de segregação de função (SoDs)
<i>Role</i>	Além de conter um Perfil de Autorização, a Role também pode conter menus iniciais customizados e outras informações ou privilégios adicionais. É tipicamente a Role que é atribuída ao usuário, fazendo com que ele ganhe acesso aos recursos contidos nas Autorizações da mesma.

<i>Rule Set</i> (Matriz de Risco)	O conjunto universo de Riscos, Regras e Funções. São tipicamente customizados para satisfazer as necessidades encontradas no cenário específico de uma determinada companhia.
SAP ERP	Sistema integrado de gestão empresarial criada pela companhia alemã SAP SE.
SAP GRC	Pacote de aplicações criada pela SAP para atender as necessidades do mercado em relação à GRC.
SAP GRC Access Control (GRC AC)	Módulo voltado ao controle de acesso do SAP GRC.
SCM	Do inglês <i>Supply Chain Management</i> , define os softwares voltados à gestão da cadeia de suprimentos.
SOx	Também conhecida como projeto de lei Sarbanes-Oxley, tem como função regulamentar os procedimentos de governança, mitigando riscos de negócio e evitando fraudes financeiras de modo a garantir transparência e integridade nos relatórios financeiros.
<i>T-code</i>	O código que cada transação possui para poder ser acessada rapidamente através do <i>menu</i> inicial. Em certos contextos, também pode referir-se à própria transação.
Transação	Uma aplicação dentro do sistema SAP, acessível via <i>menu</i> ou diretamente no <i>prompt</i> via T-code.
<i>User Authorization Buffer</i>	Nome técnico dado à área de memória reservada a cada usuário para a entrada dos dados de Autorização contidos em seus Perfis.
<i>User Profile</i> (Perfil de Usuário)	Conjunto de Roles e Perfis atribuídos a um usuário.