

# Risk Manager

## Solução Global de GRC

**Patrick Faria Coura**

[pfaria@modulo.com.br](mailto:pfaria@modulo.com.br)

# Soluções de GRC



ulo – Copyright © All rights reserved

## Projetos Especiais

# Desafios de Nossos Clientes

- Entender os Riscos Operacionais, Estratégicos e de Compliance.
- Integração de soluções para Salas de Situação
- Definir a melhor estratégia para tratamento dos Riscos encontrados.
- Garantir *Compliance* com diversas Normas e regulamentações.
- Integrar diversas ações de GRC isoladas.
- Evitar retrabalho e automatizar ações de GRC.
- Acompanhar planos de ação.
- Implementar solução de Gestão de Riscos integrada ao negócio.

## Vantagens do Risk Manager GRC

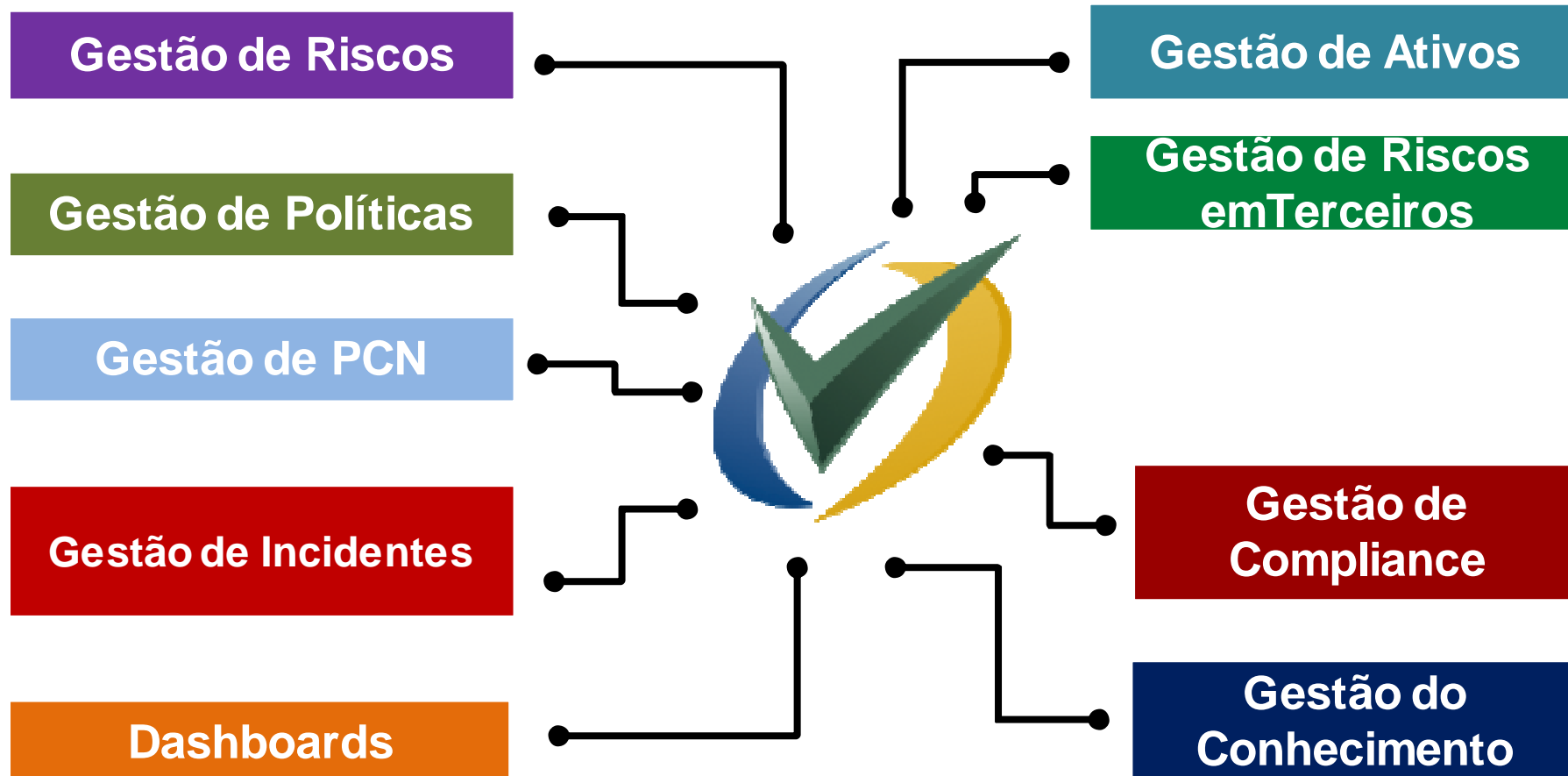
- Automatização do processo manual de GRC.
- Integração de processos fragmentados de GRC.
- Compliance com múltiplas regulamentações.
- Identificação e tratamento de Riscos de IT e de toda a Organização.
- Redução de custos com infraestrutura de IT e retrabalho.

# A Próxima Geração de Software GRC



Modulo - Copyright © All rights reserved

# Solução Risk Manager



Modulo - Copyright © All rights reserved

# Integração do GRC

## Preventivo

- SI
- Fiscalizações
- Vistorias
- ...



## Corretivo

- Eventos
- Incidentes
- ...

Modulo - Copyright © All rights reserved

# Características Gerais do Sistema

1. Full Web

2. Meu Espaço

3. Multilíngua

4. Perfis Customizáveis

The screenshots show the user interface of the MODULO Risk Manager system. The top screenshot shows the main dashboard with a sidebar and a main content area. The second screenshot shows the 'Meu Espaço' (My Space) section with a user profile and a 'Dados Pessoais' (Personal Data) section. The third screenshot shows the 'Idiomas' (Languages) section with a dropdown menu for selecting a language. The fourth screenshot shows the 'Política de Autorização' (Authorization Policy) section, which includes a tree view of roles and a table of global administrators with their permissions.

Permissões	Área	Permissões
<input type="checkbox"/>		
<input checked="" type="checkbox"/>	Visualizar Páginas em Português	Sim
<input checked="" type="checkbox"/>	Reservar Contato	Sim
<input checked="" type="checkbox"/>	Administrar Contatos de Contato	Administração
<input checked="" type="checkbox"/>	Visualizar Log de Auditoria	Administração
<input checked="" type="checkbox"/>	Administrar Customizações	Administração
<input checked="" type="checkbox"/>	Administrar Integrações	Administração
<input checked="" type="checkbox"/>	Acessar o Módulo Administração	Administração
<input checked="" type="checkbox"/>	Acessar Espaço Online	Administração
<input checked="" type="checkbox"/>	Administrar Mensagens Corporativas	Administração
<input checked="" type="checkbox"/>	Administrar Configurações de Sistema	Administração
<input checked="" type="checkbox"/>	Visualizar Integrações de Sistema	Administração
<input checked="" type="checkbox"/>	Acessar o Módulo Meu Espaço	Meu Espaço
<input checked="" type="checkbox"/>	Administrar Alíquotas	Organização
<input checked="" type="checkbox"/>	Administrar Componentes de Projetos	Organização
<input checked="" type="checkbox"/>	Editar Componentes de Projetos	Organização

Modulo - Copyright © All rights reserved



# Características Gerais do Sistema

5. Gestão Ativos

6. Gestão Riscos

7. Compliance

8. Conhecimento

**Conhecimento**

**Conhecimento de Compliance**  
Atualize os conhecimentos para o âmbito de compliance. Documentos de referência e estudos de impacto podem ser criados ou customizados. Documentos de Referência, Estudos de Impacto.

**Conhecimento de Risco**  
Atualize os conhecimentos para o âmbito de risco. Modelos de risco, questionários, análises, fontes de ataques e OPA fazem parte dos conhecimentos necessários para o âmbito de gestão de risco em SIEM. Normativas, Boas Práticas, OPA, Análises, Estudos de Impacto.

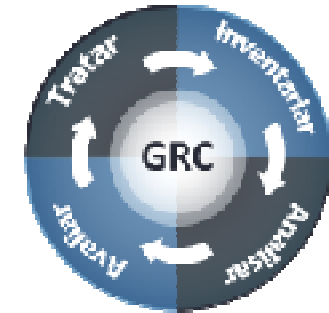
**Pesquisas**  
Crie ou edite pesquisas personalizadas para projetos de compliance e risco.

**Últimas atualizações**

Item Atualizado	Autor	Data	Situação
Conhecimento de Compliance - Documento de Referência - Documento de Referência	Verônica Zilli	26/04/2019 10:55:28	Em criação
Conhecimento de Compliance - Documento de Referência - Lista de Desempenhadores	Verônica Zilli	26/04/2019 10:55:27	Em criação
Pesquisas - Map Análise Controle e Pontos - Banco II	Verônica Zilli	26/04/2019 09:55:51	Publicado
Pesquisas - Pesquisas Manuais por Projetos - Banco II	Verônica Zilli	26/04/2019 09:55:45	Publicado
Pesquisas - Pesquisas de Análise de Normas - Banco II	Verônica Zilli	26/04/2019 10:55:04	Publicado
Conhecimento de Compliance - Documento de Referência - Lei 10.820	Verônica Zilli	26/04/2019 14:45:32	Publicado
Conhecimento de Compliance - Documento de Referência - Lei 11.890	Verônica Zilli	26/04/2019 14:45:32	Publicado
Pesquisas - Pesquisas de "Codigo de Conduta - Empresa SP2"	Verônica Zilli	12/04/2019 09:45:18	Publicado
Conhecimento de Compliance - Documento de Referência - Código de Conduta - Empresa SP2	Verônica Zilli	12/04/2019 09:45:12	Publicado
Conhecimento de Compliance - Documento de Referência - BRCC - Código das Normas Públicas de Tecnologia Corporativa	Verônica Zilli	11/04/2019 23:52:18	Publicado

Modulo - Copyright © All rights reserved

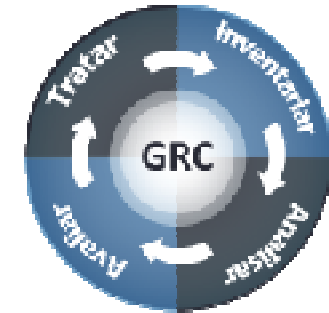
# Módulo - Gestão de Riscos



1. Análise
2. Utilização KB's
3. KB's e perguntas Customizáveis
4. Pesquisas

Modulo - Copyright © All rights reserved

# Módulo - Gestão de Riscos



5. Scanners



kp-sp2

Propriedades | Atributos Customizáveis | Histórico de Análises | Situação | Vulnerabilidades | Extrair relatório

Analise de Riscos - Abril 2010

Inventariar | Analisar | Avaliar | Tratar

Tratamento de Riscos

Estadísticas do Projeto

Indicadores de Riscos do Tratamento (PSR/Controles)

	PSR (Controles)	Risk Index	Gap Index	Residual
Não Avaliados	707 (22)	11,0%	11,0%	Risco 14,2%
Aceitos	100 (3)	2,0%	2,0%	Gap 14,2%
Em Tratamento	928 (27)	14,0%	14,2%	
Tratados	0 (0)	0,0%	0,0%	
Controlados	4764 (138)	71,7%	71,4%	

Estadísticas de Riscos do Tratamento (PSR)

Estágio	Controlado	Em Tratamento	Aceitos	Não Avaliados
Análise	61,4%	38,6%	0%	0%
Avaliação	61,4%	12,0%	2,4%	24,2%
Tratamento	61,4%	12,0%	2,4%	24,2%

6. What / If

7. Padrões

**Common Event Expression**  
A Standard Log Language for Event Interoperability in Electronic Systems



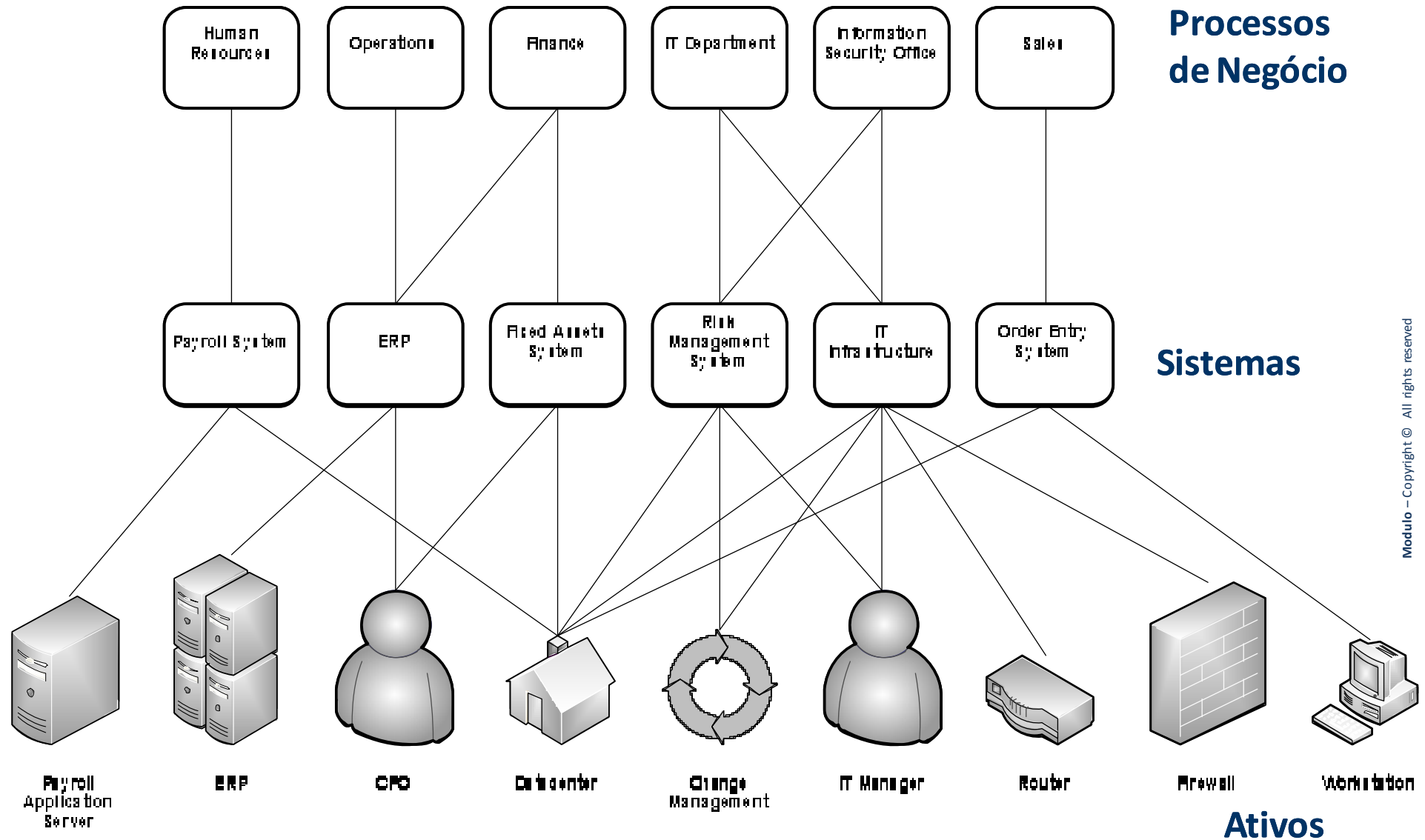
# Abordagem Top-Down “Governança”

**Processos  
de Negócio**

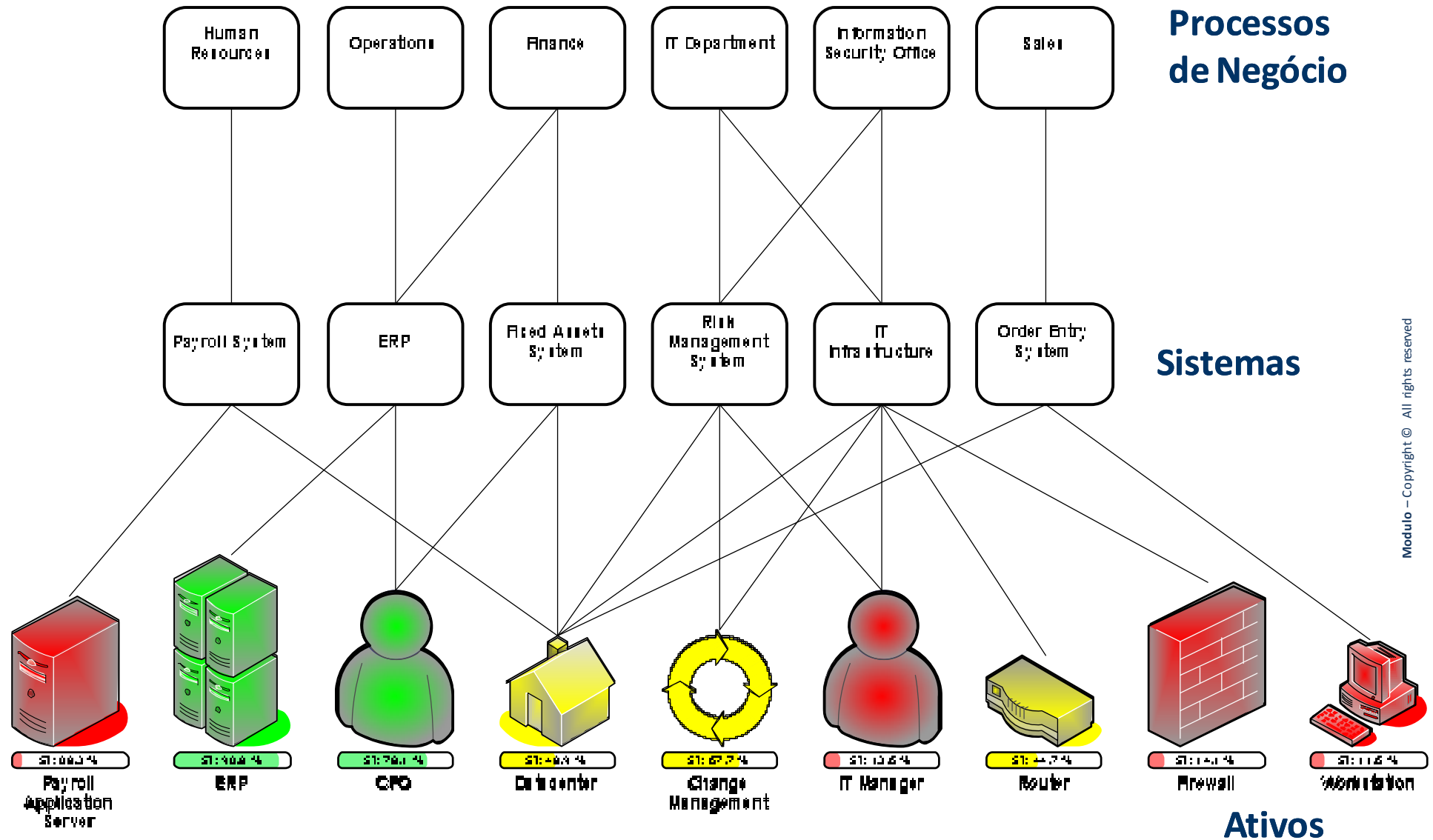
**Sistemas**

**Ativos**

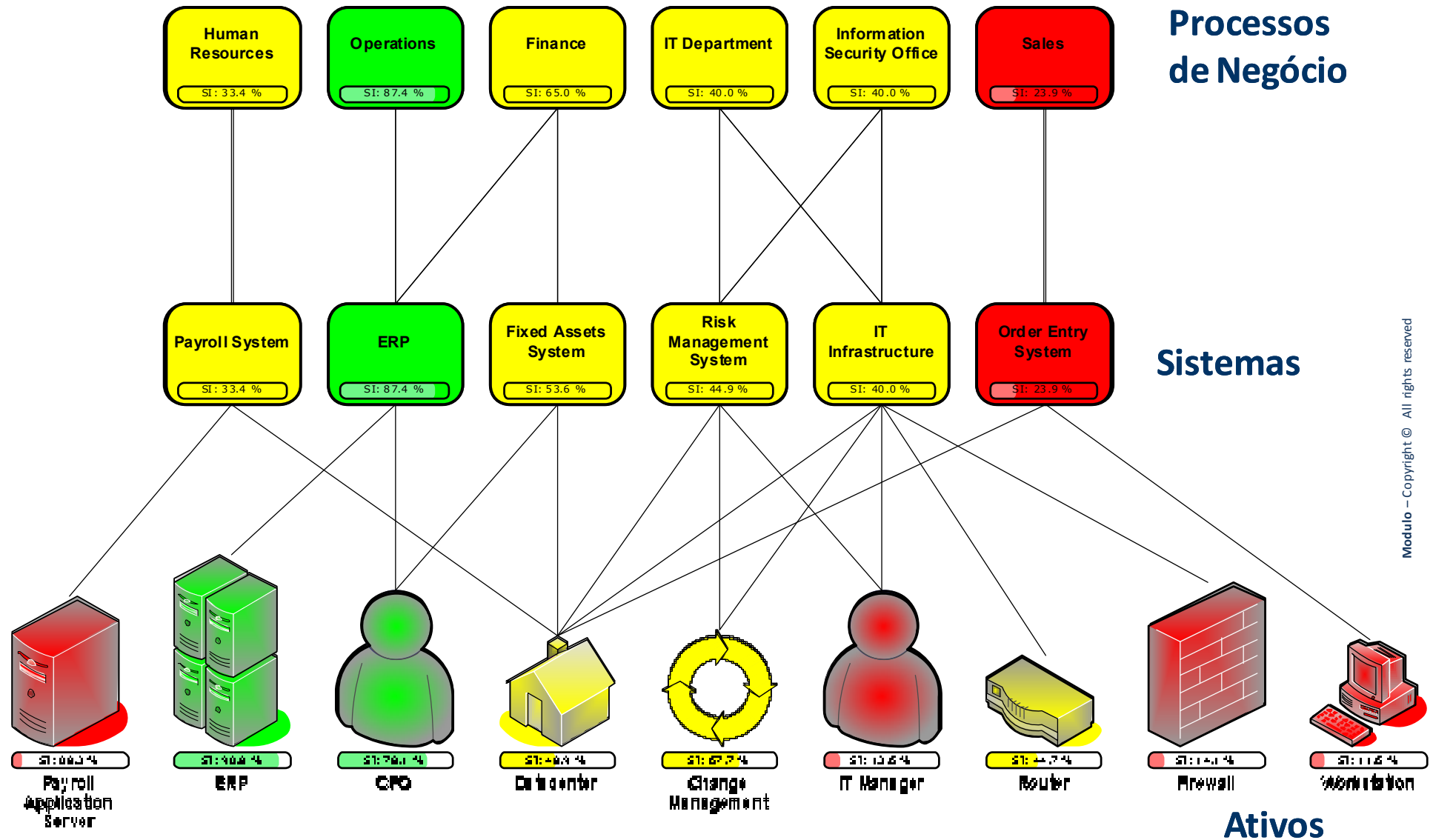
# Abordagem Top-Down “Governança”



# Abordagem Top-Down “Governança”



# Abordagem Top-Down “Governança”



# Módulo - Relatórios



### 3. Next Steps

This analysis has pinpointed the major risks in the assets. The findings of this analysis will help in the decision-making process to address situations that affect the organization's goals. The risk level and its interpretation for each possible amount are suggested in the table below:

Risk Level	Definition	Point Values
Very High	Not acceptable risks. The entire organization could be seriously affected and the damage or losses would be extremely high. Assets Managers should be oriented to eliminate them.	60, 64, 75, 86, 100, 125
High	Not acceptable risks. One or more business processes could be seriously affected and the damage or losses would be very high. Assets managers should be oriented to control them.	32, 36, 40, 43, 46, 50
Medium	Risks that can be acceptable after assets managers review and acceptance. Part of the business could be affected and the damage or losses would be noticeable. This process should be done by formal means.	18, 20, 24, 25, 27, 30
Low	Risks that can be acceptable after assets managers review and acceptance. A small and well-defined part of the business would be affected and the damage or losses would be low.	8, 9, 10, 12, 15, 16
Very Low	Acceptable risks that should be reported to assets managers.	1, 2, 3, 4, 5, 6

ID	Control	Asset	Knowledge Base	PSR	Status	History
225	NTFS permissions for the "%SystemRoot%\system32\regedit32.exe" file should be set up to prevent unauthorized access.	Operating System - "Microsoft" - MS Windows Srv 2003 v5.90	Operating System - "Microsoft" - MS Windows Srv 2003			
226	The "Modify firmware environment values" parameter should be set as follows: "Administrators".	Operating System - "Microsoft" - MS Windows Srv 2003 v5.90	Operating System - "Microsoft" - MS Windows Srv 2003			
227	NTFS permissions for the "%SystemRoot%\system32\lsass.exe" file should be set up to prevent unauthorized access.	Operating System - "Microsoft" - MS Windows Srv 2003 v5.90	Operating System - "Microsoft" - MS Windows Srv 2003			
228	The "Profile system performance" parameter should be set as follows: "Administrators".	Operating System - "Microsoft" - MS Windows Srv 2003 v5.90	Operating System - "Microsoft" - MS Windows Srv 2003			
229	NTFS permissions for the "%SystemRoot%\system32\lsass.exe" file should be set up to prevent unauthorized access.	Operating System - "Microsoft" - MS Windows Srv 2003 v5.90	Operating System - "Microsoft" - MS Windows Srv 2003			
230	The "Remove computer from docking station" parameter should be set as follows: "No user".	Operating System - "Microsoft" - MS Windows Srv 2003	Operating System - "Microsoft" - MS Windows Srv 2003			

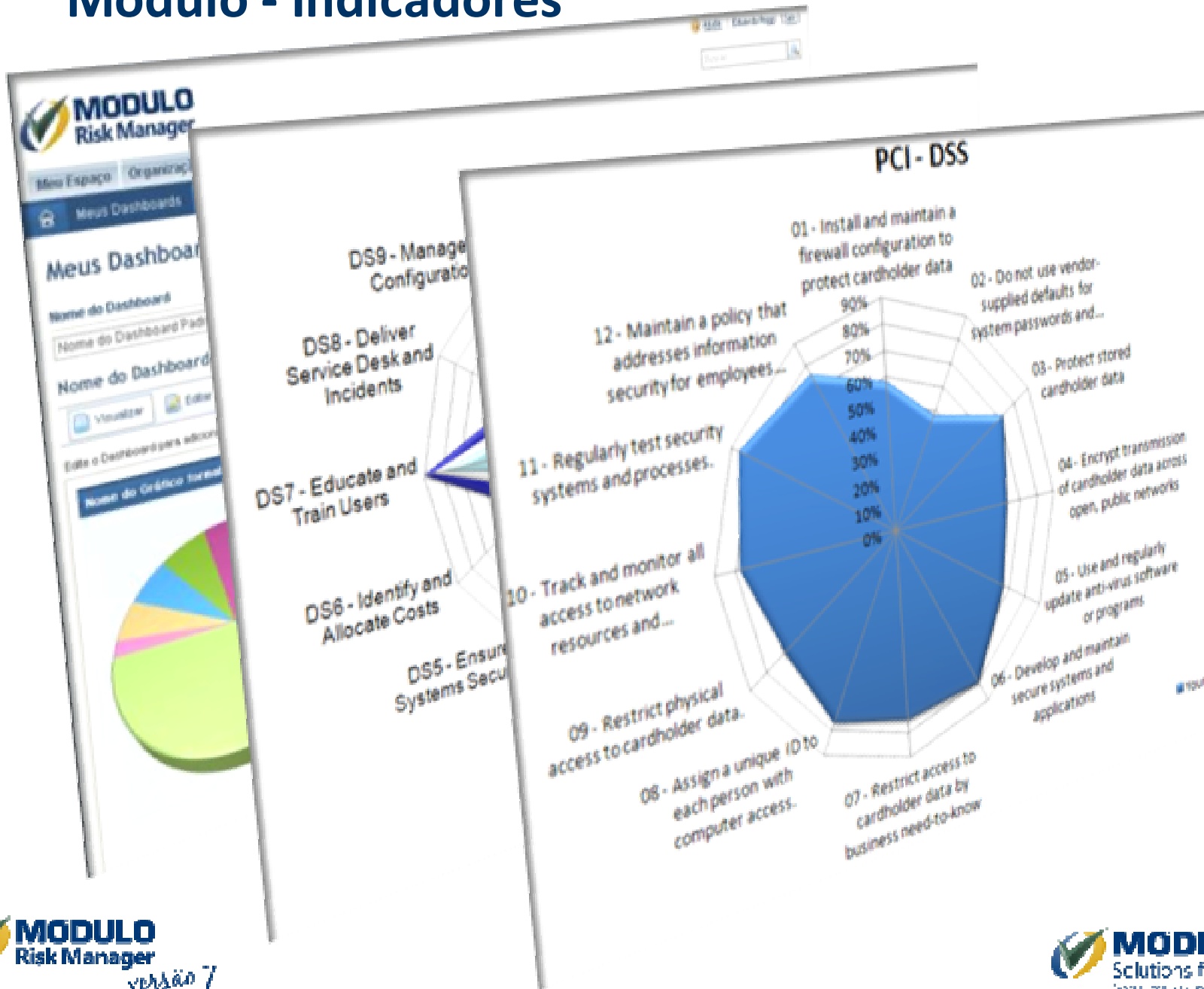
### 2.5.1. Risks per Business Component

The following table shows the consolidated indexes by first-level business components (Strategical Level). It shows the absolute and percentage amounts of risks for the 10 components having the highest risk index.

BUSINESS PROCESS	RELEVANCE	IMPLEMENTED CONTROLS	HIGH-IMPLEMENTED CONTROLS	CONTROL INDEX	GAP INDEX	AVOIDED RISKS	IDENTIFIED RISKS	SECURITY INDEX	RISK INDEX
Human Resources	Average	293	153	65.70%	34.30%	9306	5226	64.04%	35.96%
Operations	Average	293	153	65.70%	34.30%	9306	5226	64.04%	35.96%
Sales	Average	328	163	66.80%	33.20%	10344	5496	65.30%	34.70%
Information Security Office	Average	349	163	68.16%	31.84%	10944	5496	66.57%	33.43%
Finance	Average	335	153	68.65%	31.35%	10506	5226	66.78%	33.22%
IT Department	Average	370	163	69.42%	30.58%	11544	5496	67.75%	32.25%



# Módulo - Indicadores



# Módulo - Visão Integrada com o Negócio

**MODULO Risk Manager**

## Visão Integrada de Componente de Negócio

**Business Components Operational layer**

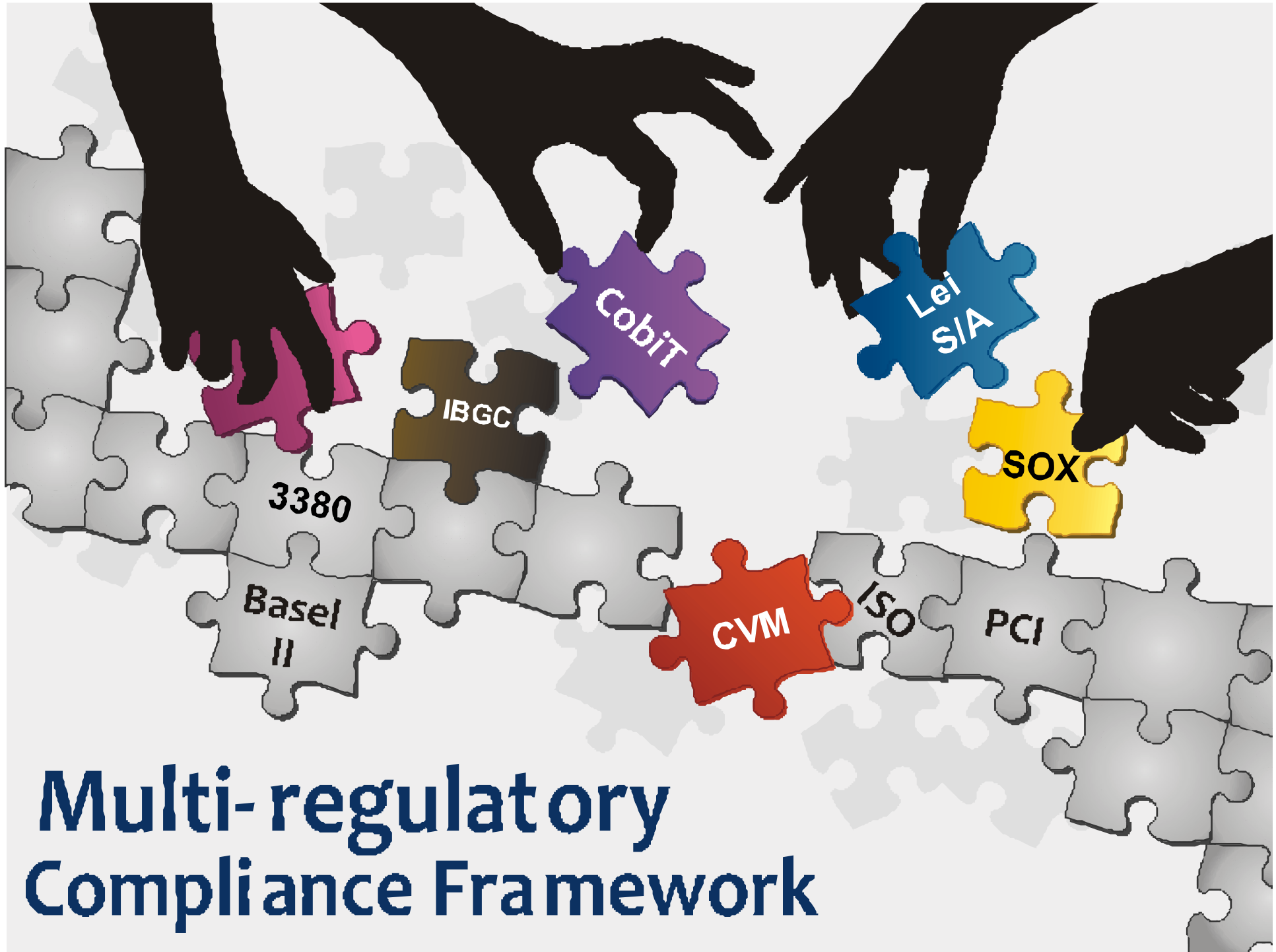
### Network Services

Description

Associations

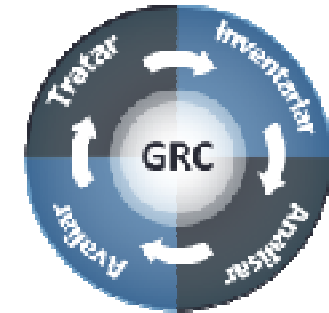
Name
Strategic Vision
Service Delivery
Customer Relations
Manage Finances

Name
Notebook - Consultant - BRA
Consultant - BRA
Operations - USA
Operations - BRA
Datacenter
Notebook - Analyst Development - BRA
Notebook - Manager Development -



# Multi-regulatory Compliance Framework

# Módulo - Compliance



Requisito	Compliance Limit	Indicador
016.009.009.014.014.015.010.009.014.014.015.011.012.019.011.016.013.016.0	0,00%	Not Applicable
016.009.009.014.014.015.010.009.014.014.015.011.012.019.011.016.013.016.0	0,00%	Not Applicable
016.009.009.014.014.015.010.009.014.014.015.011.012.019.011.016.013.016.0	0,00%	Not Applicable
016.009.009.014.014.015.010.009.014.014.015.011.012.019.011.016.013.016.0	0,00%	Not Applicable
016.009.009.014.014.015.010.009.014.014.015.011.012.019.011.016.013.016.0	0,00%	Not Applicable
016.009.009.014.014.015.010.009.014.014.015.011.012.019.011.016.013.016.0	0,00%	Not Applicable
016.009.009.014.014.015.010.009.014.014.015.011.012.019.011.016.013.016.0	0,00%	Not Applicable
016.009.009.014.014.015.010.009.014.014.015.011.012.019.011.016.013.016.0	0,00%	Not Applicable
016.009.009.014.014.015.010.009.014.014.015.011.012.019.011.016.013.016.0	0,00%	Not Applicable
016.009.009.014.014.015.010.009.014.014.015.011.012.019.011.016.013.016.0	0,00%	Not Applicable

1. Documentos de Referência

2. Referência Cruzada

3. Multi Regulatório

4. Busca Avançada

5. Índices de não Conformidade

Modulo - Copyright © All rights reserved

# Módulo - Tratamento de Riscos e Não Conformidades

## Workflow

### Eventos

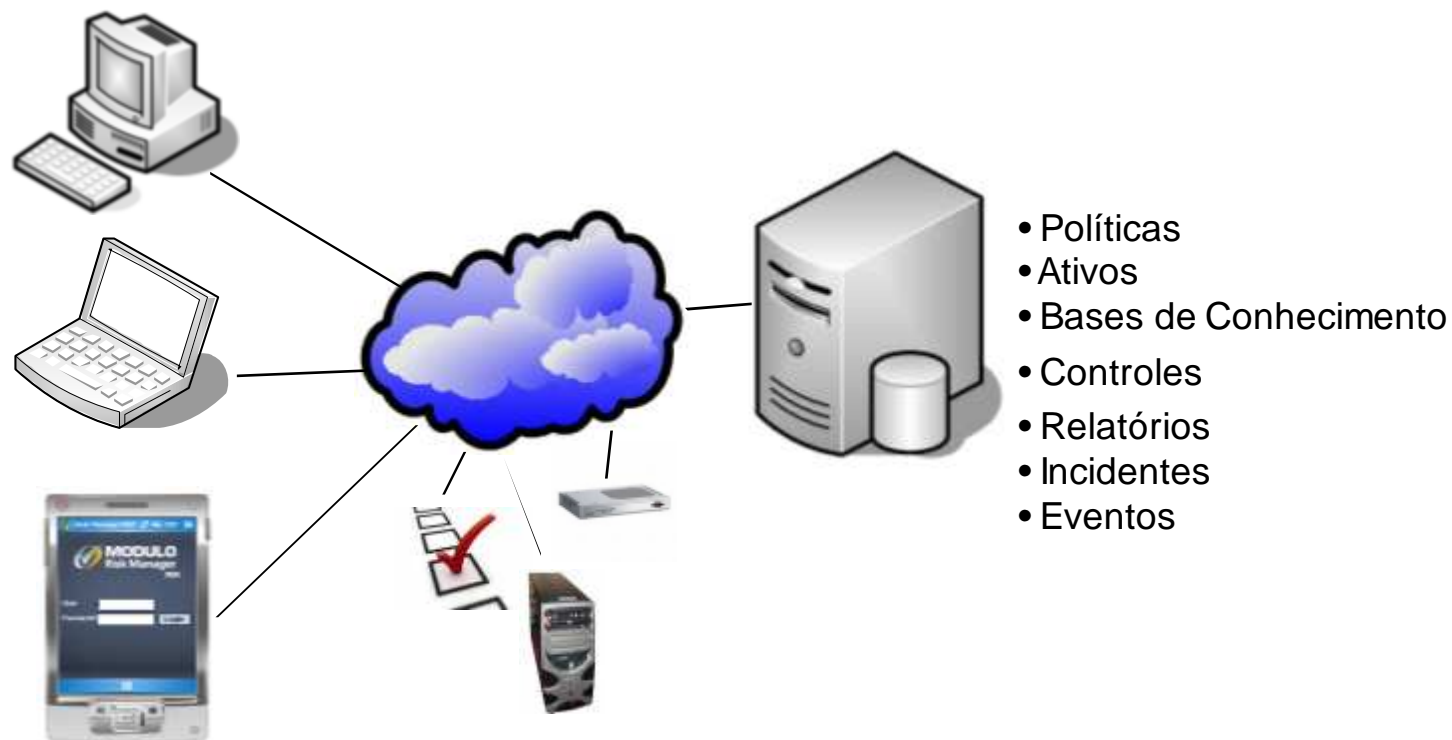
<span>📄 Criar Evento</span> <span>🗑️ Fechar Evento</span> <span>🗑️ Cancelar Evento</span> <span>🔍 Reabrir Evento</span> <span>🔄 Atualizar Progresso</span> <span>⚙️ Configurar Colunas</span> <span>📄 Exportar ▾</span>													
<input type="checkbox"/>			ID	USR	Progresso	Título	Tipo	Origem	Situação	Coordenador	Responsável	Subordinado	Prazo
		Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	Filtro	▾	Filtro	Filtro	Filtro	Filtro ▾
<input type="checkbox"/>			EVTR201004000020	45	100%	O dispositivo de controle de temperatura do Data Center deve ser instalado fora do alcance das pessoas.	Evento de Risco	PRJR10004	Fechado	Administrator	Administrator		30/8/2010
<input type="checkbox"/>			EVTC201004000059	1	0%	7.4 Organização para gestão de riscos de segurança da informação	Evento de Compliance	PRJC10003	Aberto	Administrator	Administrator		16/4/2010
<input type="checkbox"/>			EVTR201004000068	45	0%	O componente é vital para a empresa, considerando a integração estratégica com o negócio	Evento de Risco	PRJR10001	Aberto	Administrator	Administrator		
<input type="checkbox"/>			EVTC201004000065	1	0%	3.8 retenção do risco	Evento de Compliance	PRJC10003	Aberto	Administrator	Administrator		16/4/2010
<input type="checkbox"/>			EVTR201004000074	45	0%	O componente é muito eficiente, atuando de forma normal em termos de demanda x produção e com flexibilidade para incrementos ou decrementos de sua produção conforme a demanda	Evento de Risco	PRJR10001	Aberto	Fernando Nery	Fernando Nery		
<input type="checkbox"/>			EVTC201004000069	1	0%	2.12 Convidados para as reuniões do Conselho	Evento de Compliance	PRJC10003	Aberto	Administrator	Administrator		
<input type="checkbox"/>			EVTR201004000004	45	0%	Exercícios de simulação de incêndios devem ser realizados periodicamente pelas pessoas que trabalham no ambiente.	Evento de Risco	PRJR10004	Aberto	Administrator	Administrator		17/11/2010
<input type="checkbox"/>			EVTR201004000043	45	100%	Os terceiros devem ser acompanhados por pessoas autorizadas no acesso ao Data Center.	Evento de Risco	PRJR10004	Fechado	Administrator	Administrator		22/9/2010
<input type="checkbox"/>			EVTR201004000052	45	100%	Um sistema de refrigeração exclusivo deve ser instalado no Data Center.	Evento de Risco	PRJR10004	Fechado	Administrator	Administrator		23/9/2010
<input type="checkbox"/>			EVTR201004000017	45	60%	Detectores de fogo e fumaça devem ser instalados abaixo do piso elevado do Data Center.	Evento de Risco	PRJR10004	Aberto	Administrator	Administrator		30/8/2010

Página 1 de 8 (74 itens) ⏪ [1] 2 3 4 5 6 7 8 ⏩

🔍 Criar Filtro

# Arquitetura da Solução

- Solução de GRC totalmente compatível com Cloud Computing
- Arquitetura distribuída
- Controle de Acesso granular.
- Login de qualquer lugar.
- Acessível de diversos devices.



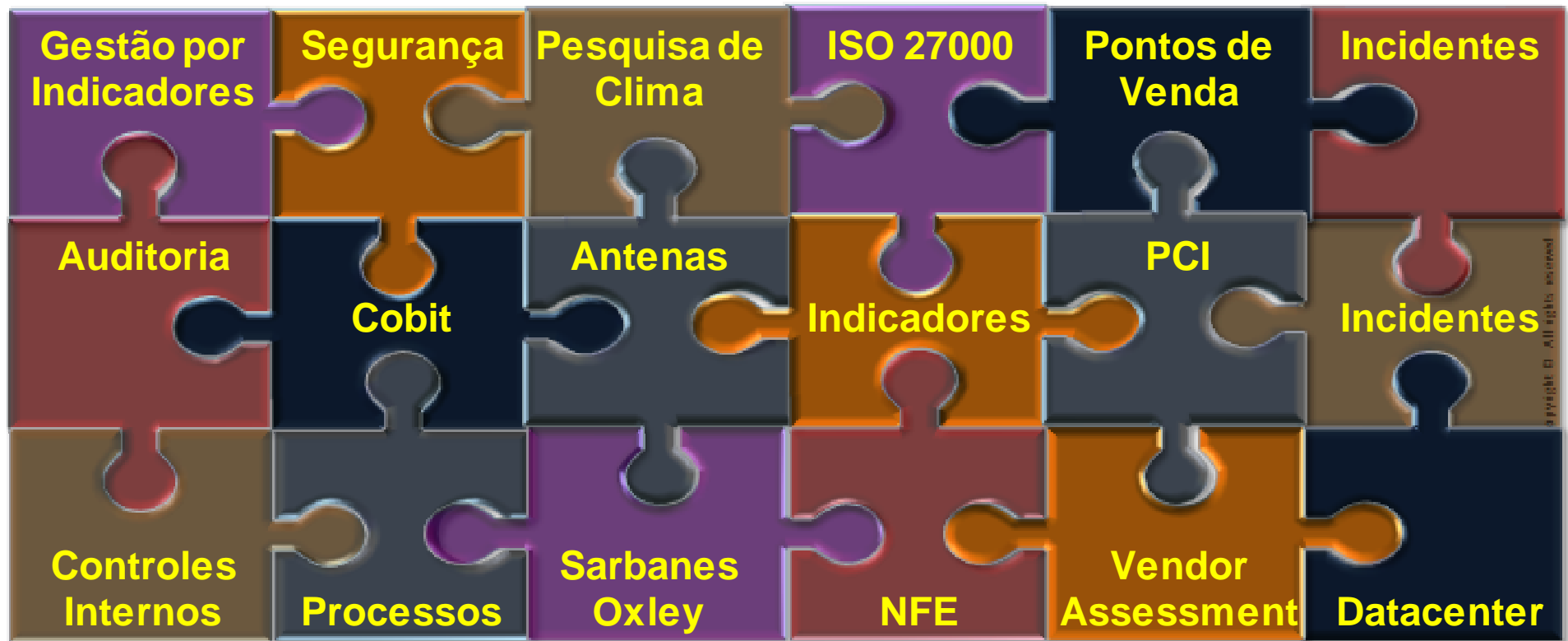
Modulo – Copyright © All rights reserved

# Modelos para Instalação

- Appliance
- Ambiente dedicado do cliente
- SaaS

Um único software

... diversas aplicações!





# Obrigado

**Patrick Faria Coura**

[pfaria@modulo.com.br](mailto:pfaria@modulo.com.br)