MÓDULO Solutions for GRC | Governance, Risk and Compliance

IBM Security Forum
Soluções para um ambiente seguro

Gestão de Riscos no contexto da NBR ISO/IEC 27005

Alberto Bastos, CISSP, MCSO
abastos@modulo.com.br

Sócio-Fundador da Módulo
Coordenador da CEE Gestão de Riscos ABNT

1ª Empresa de Segurança da Informação certificada ISO 27001 no mundo

CERTIFICADA ISO 9001 BSI

MÓDULO Risk Manager

MODULO
Solutions for GRC

ISO
IEC

ISO
International
Organization for
Standardization

CERTIFICADA
ISO 9001

IBM Security Forum
Soluções para um ambiente seguro

MÓDULO
Solutions for GRC

Development of standards for the protection of information and ICT.

SC27: IT Security Techniques

Série ISO/IEC 27000

Standard	Description	Phase
27000	Overview and Vocabulary	FDIS
27001	Requirements	Published 2005
27002	Code of practice	Published 2005
27003	Implementation Guidance	DIS
27004	Measurements	DIS
27005	Information Security Risk Management	Published 2008
27006	Guidelines for the Acreditation of Bodies	Published 2007
27007	Guidelines for auditing	WD

NBR – Norma Brasileira

MÓDULO
Solutions for GRC

NBR

ISO/IEC 27005

Escopo

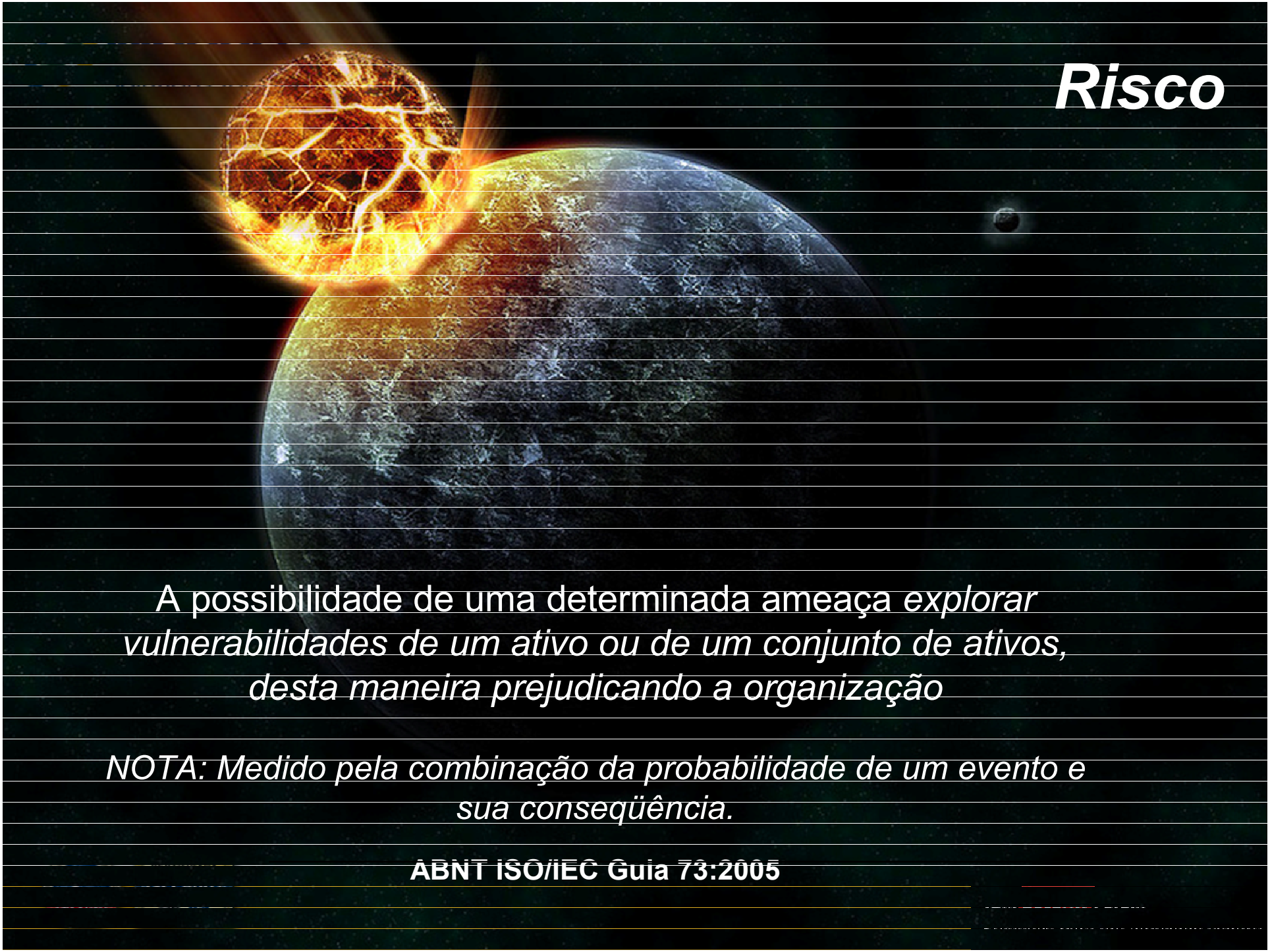
Diretrizes para gestão de riscos de segurança da informação...
... de acordo com a ABNT NBR ISO/IEC 27001...
... facilita a implementação satisfatória da segurança da informação tendo como base a gestão de riscos.

... se aplica a todos os tipos de organização.

Termos e Definições

Impacto
Mudança adversa no nível obtido dos objetivos de negócios

Risco



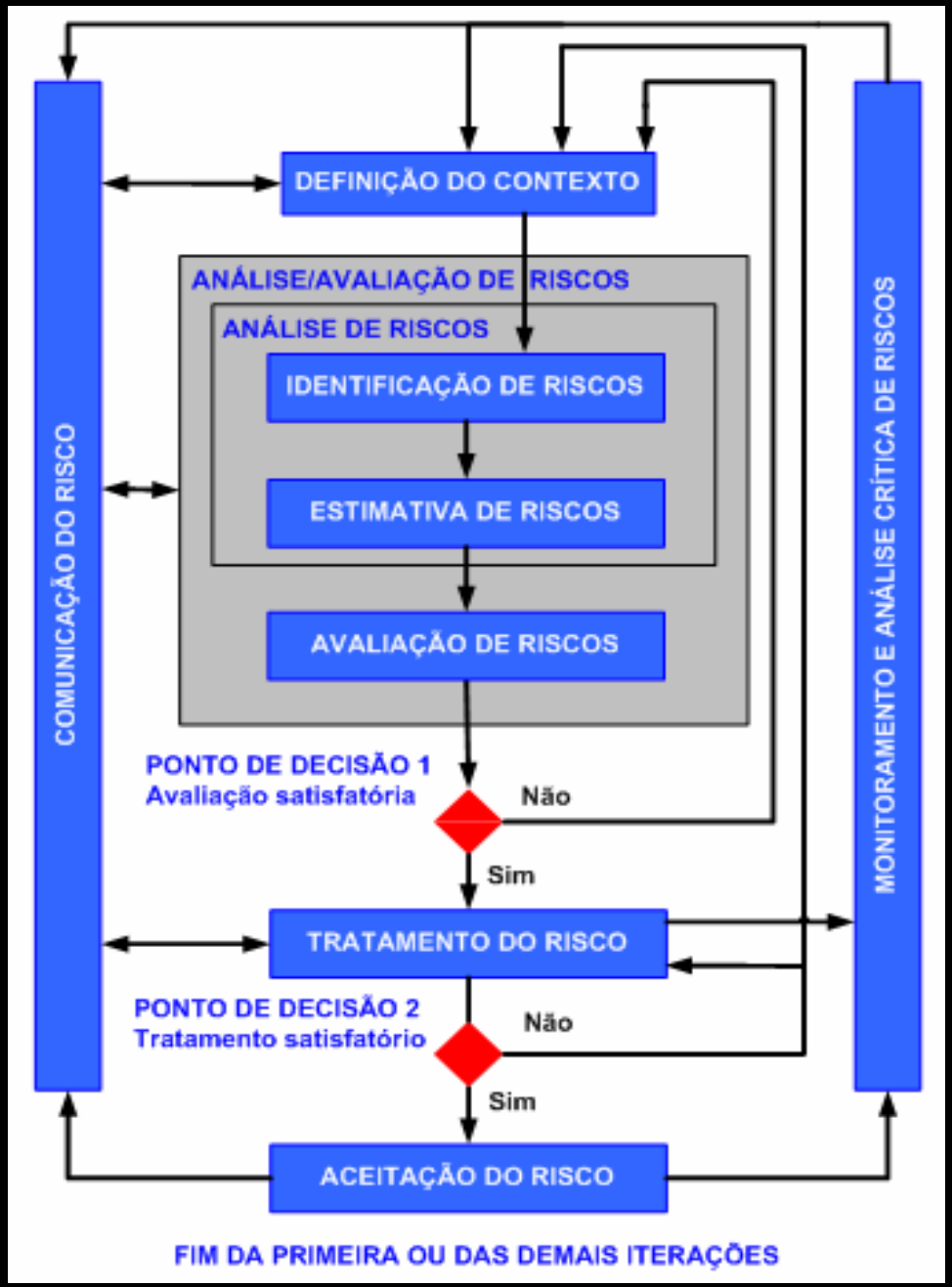
A possibilidade de uma determinada ameaça *explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira prejudicando a organização*

NOTA: Medido pela combinação da probabilidade de um evento e sua conseqüência.

ABNT ISO/IEC Guia 73:2005

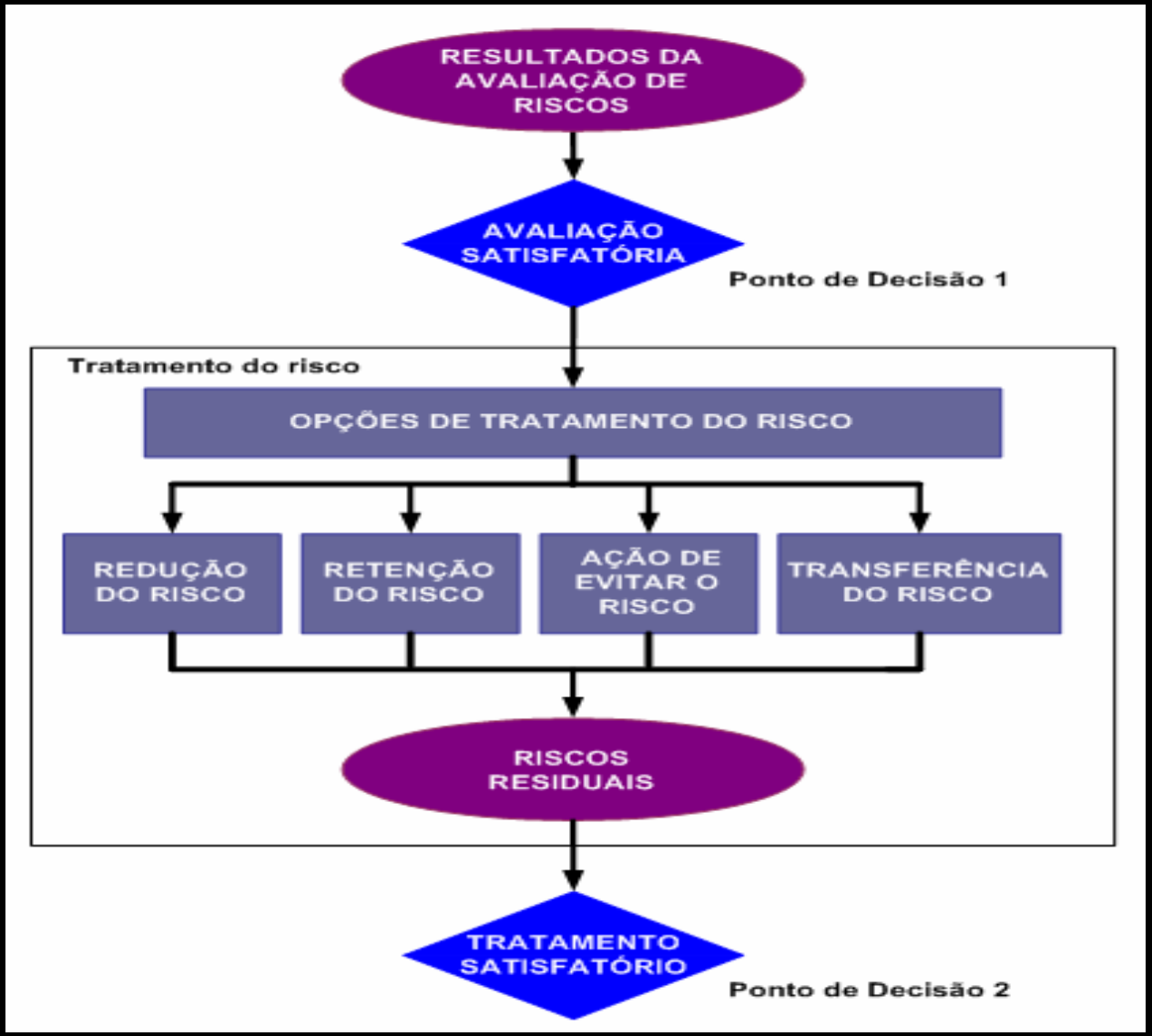
Visão Geral 27005

(Organização da norma)



. Visão geral do processo
. Definição do contexto
. Análise/avaliação de riscos
. Tratamento do risco
. Aceitação do risco
. Comunicação do risco
. Monitoramento e análise crítica de riscos
. ANEXOS

Tratamento do Risco




Para onde vamos?

Disco rígido de 5MB,
lançado pela IBM em 1956
no primeiro computador
com Hard Disk, pesava 1 tonelada!

ORÇAMENTO DA SEGURANÇA

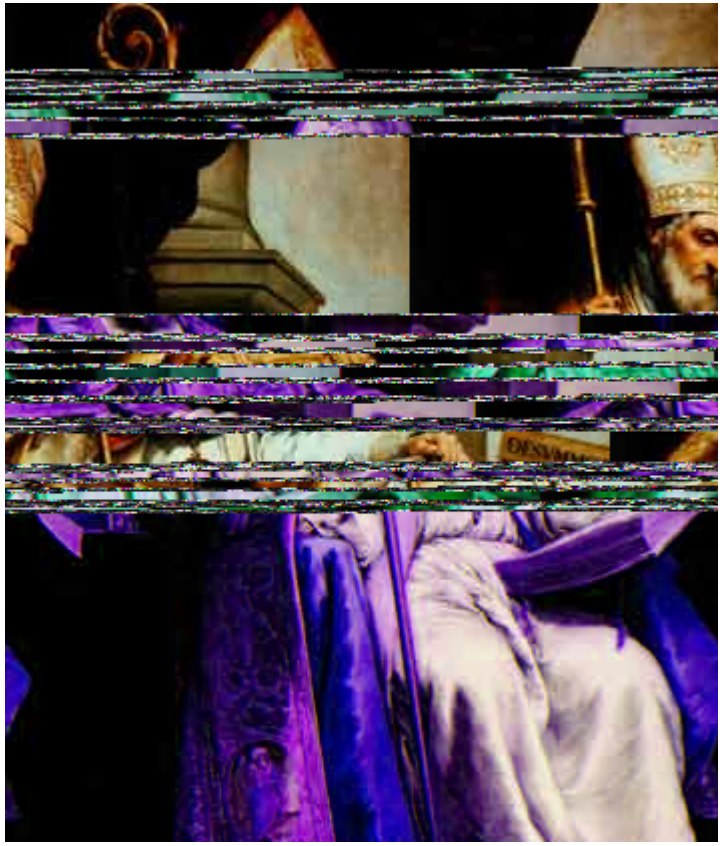
Information Security Governance

"Nunca na história tivemos tão formidável tecnologia. Todo o avanço científico conhecido pela humanidade foi incorporado no projeto. Os controles operacionais são a prova de falhas!"

E.J. Smith, Captain of the Titanic

Fé X Confiança

Santo Isidoro de Sevilha



Oração para antes da ligação à Internet

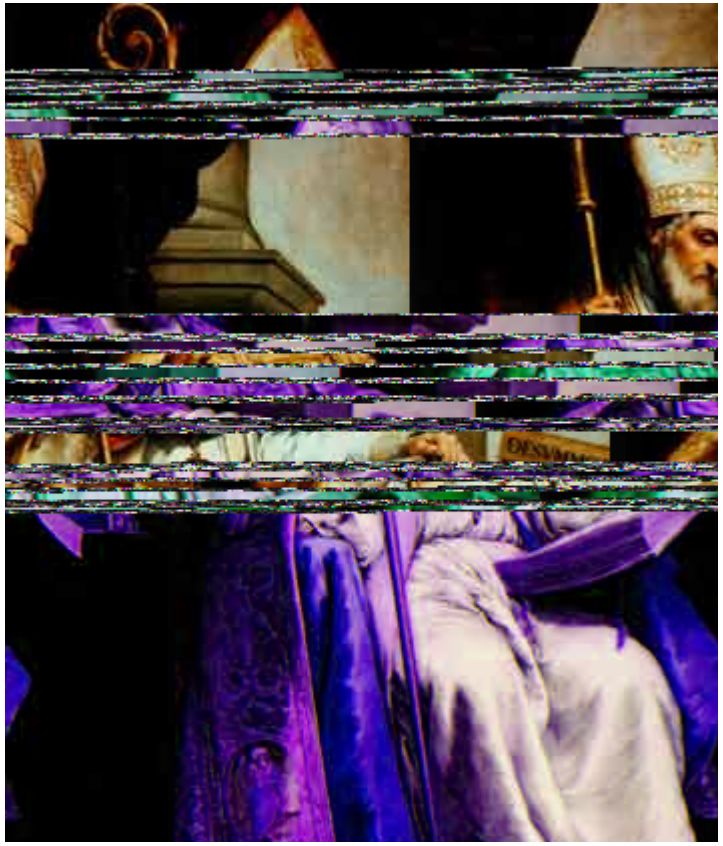
Deus Todo-Poderoso e eterno, que nos criastes à vossa imagem e nos mandastes buscar tudo quanto é bom, verdadeiro e belo, ...

Nós Vos pedimos, que por intercessão de Santo Isidoro, que durante nossas viagens na Internet movamos nossas mãos e nossos olhos para somente ao que Vos agrada, e que tratemos com caridade e paciência todos as almas que encontrarmos.

Por Jesus Cristo Nosso Senhor. Amém.

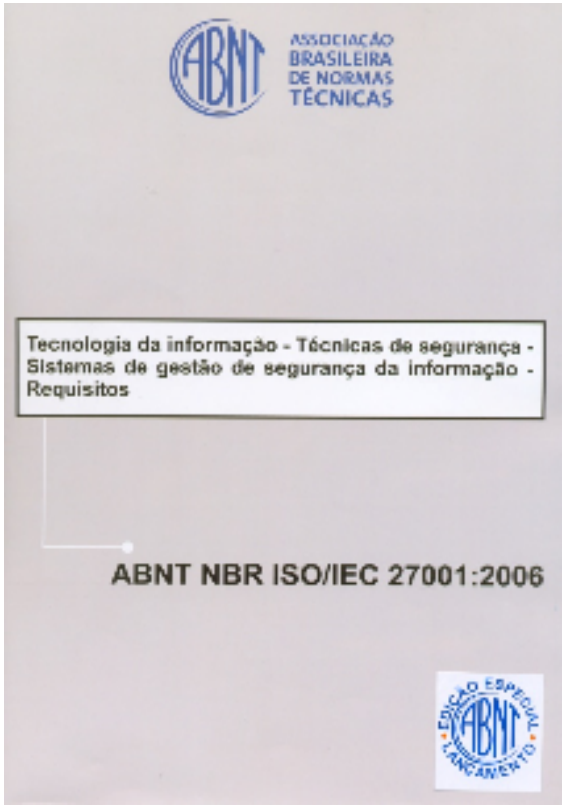
Fé X Confiança

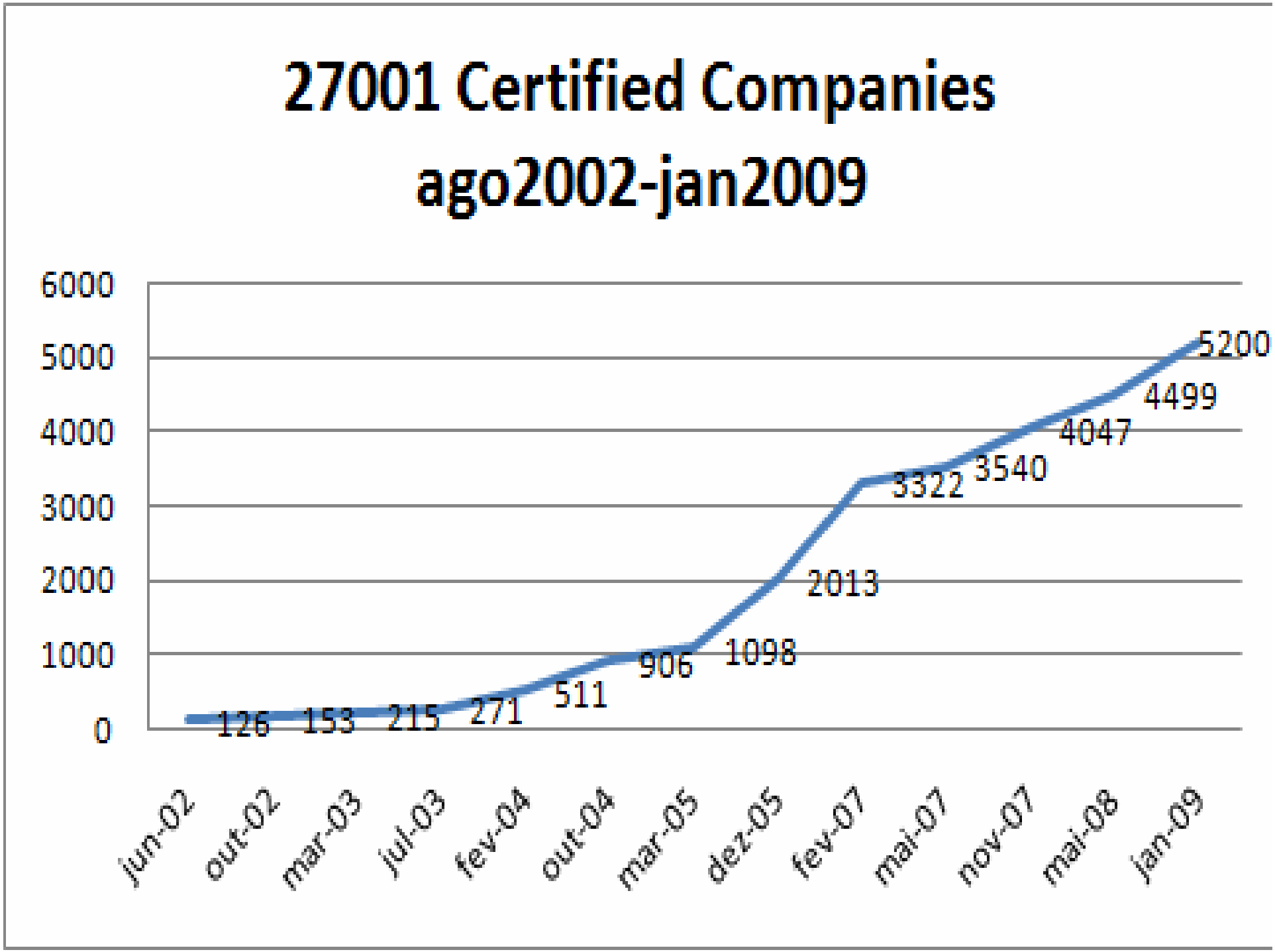
Santo Isidoro de Sevilha



vs

NBR ISO 27001




27001 Certified Companies
ago2002-jan2009
6000
5000
4000
3000
2000
1000
0
126
153
215
271
511
906
1098
2013
3322
3540
4047
4499
5200
jun-02
out-02
mar-03
jul-03
fev-04
out-04
mar-05
dez-05
fev-07
mai-07
nov-07
mai-08
jan-09

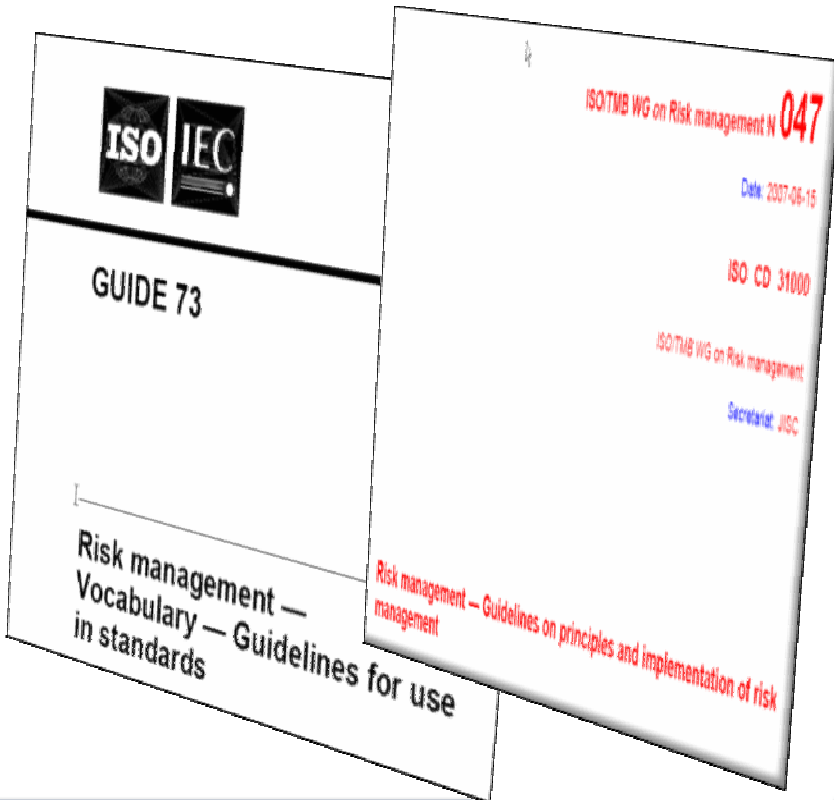
Number of Certificates Per Country

Japan	2994*	Netherlands	11	Gibraltar	4
India	440	Pakistan	11	Bulgaria	3
UK	374	Singapore	11	Oman	3
Taiwan	210	France	10	Bangladesh	2
China	182	Philippines	10	Canada	2
Germany	108	Saudi Arabia	10	Isle of Man	2
USA	85	Russian Federation	10	Morocco	2
Czech Republic	78	Greece	9	Qatar	2
Hungary	78	Slovenia	7	Yemen	2
Korea	74	Sweden	7	Armenia	1
Italy	55	Slovakia	6	Belgium	1
Hong Kong	38	South Africa	6	Egypt	1
Poland	35	Colombia	5	Iran	1
Australia	28	Croatia	5	Kazakhstan	1
Spain	27	Indonesia	5	Kyrgyzstan	1
Austria	26	Bahrain	4	Lebanon	1
Ireland	26	Kuwait	4	Lithuania	1
Malaysia	26	Norway	4	Luxembourg	1
Brazil	21	Sri Lanka	4	Macedonia	1
Thailand	21	Switzerland	4	Moldova	1
Mexico	20	Chile	3	New Zealand	1
Romania	19	Macau	3	Ukraine	1
Turkey	15	Peru	3	Uruguay	1
UAE	15	Portugal	3	Relative Total	5200
Iceland	11	Vietnam	3	**Absolute Total**	**5190**

ISO 31000

- *ISO 31000: Principles and Guidelines on Risk Management*
- *ISO Guide 73: Concepts and Vocabulary*

- Cingapura Meeting – Nov/2008
- Lançamento em 2009

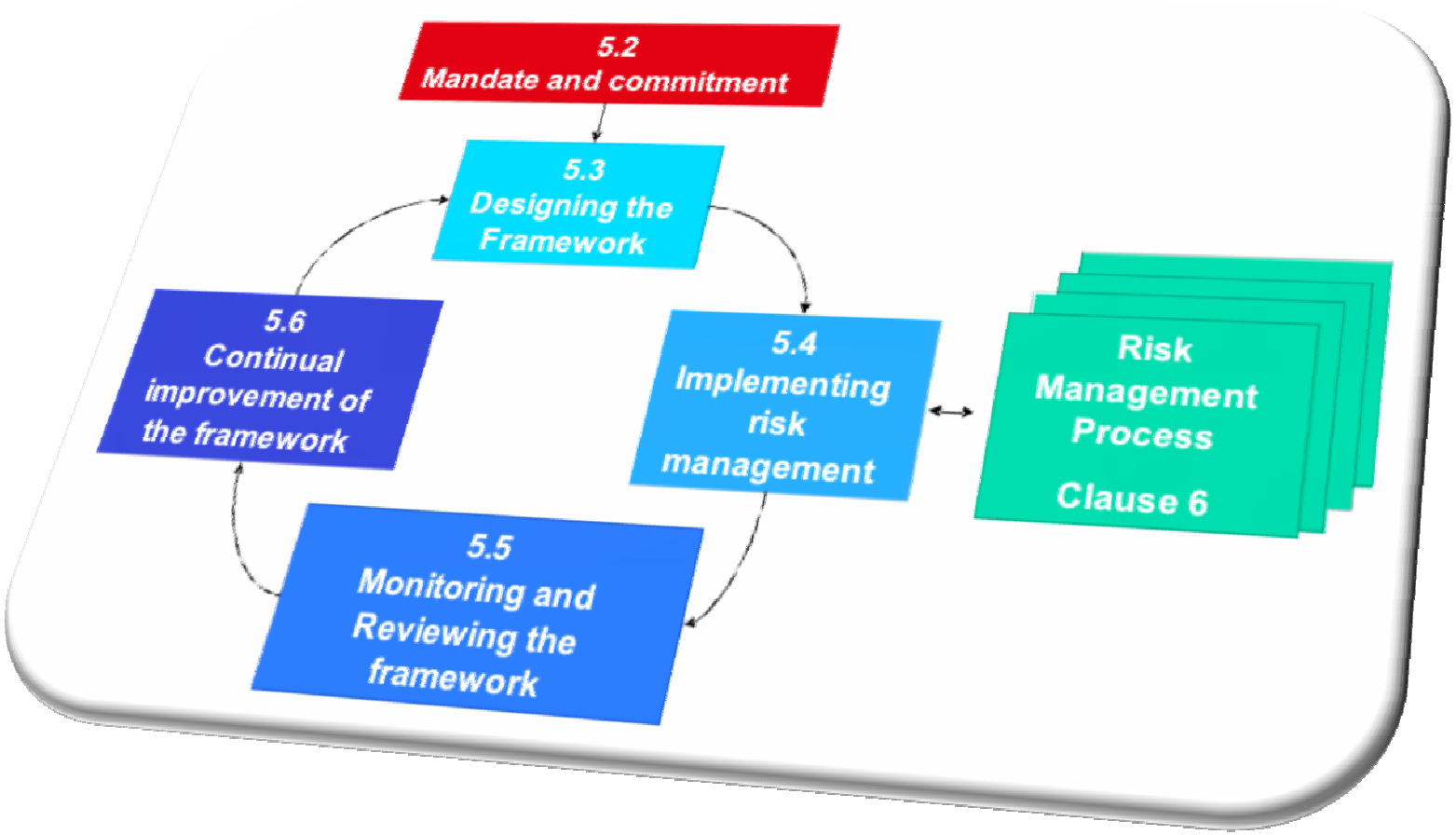


MÓDULO
Solutions for GRC

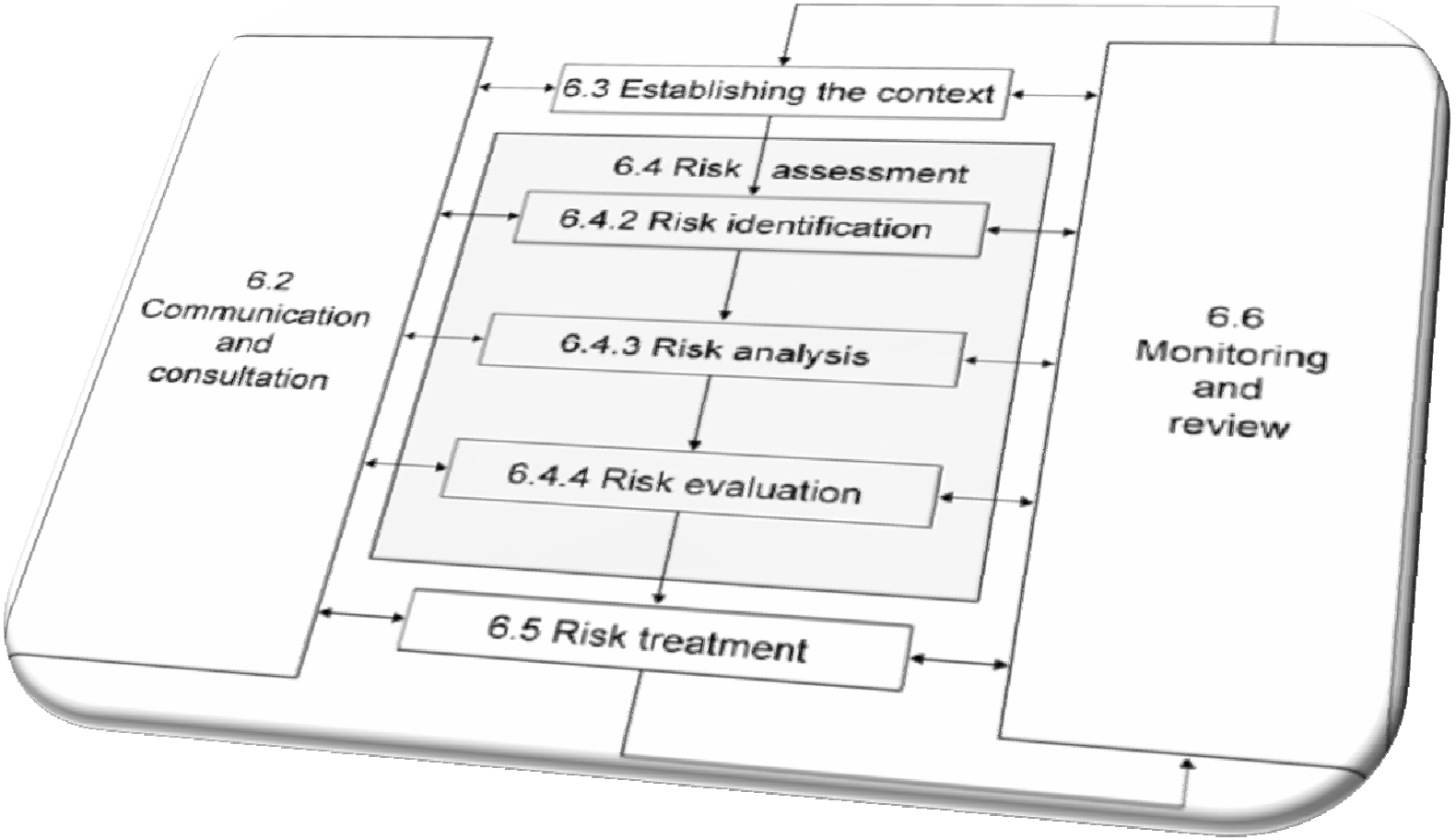
Gestão de Riscos nas organizações

"Atividades coordenadas para dirigir e controlar uma organização com relação ao risco"

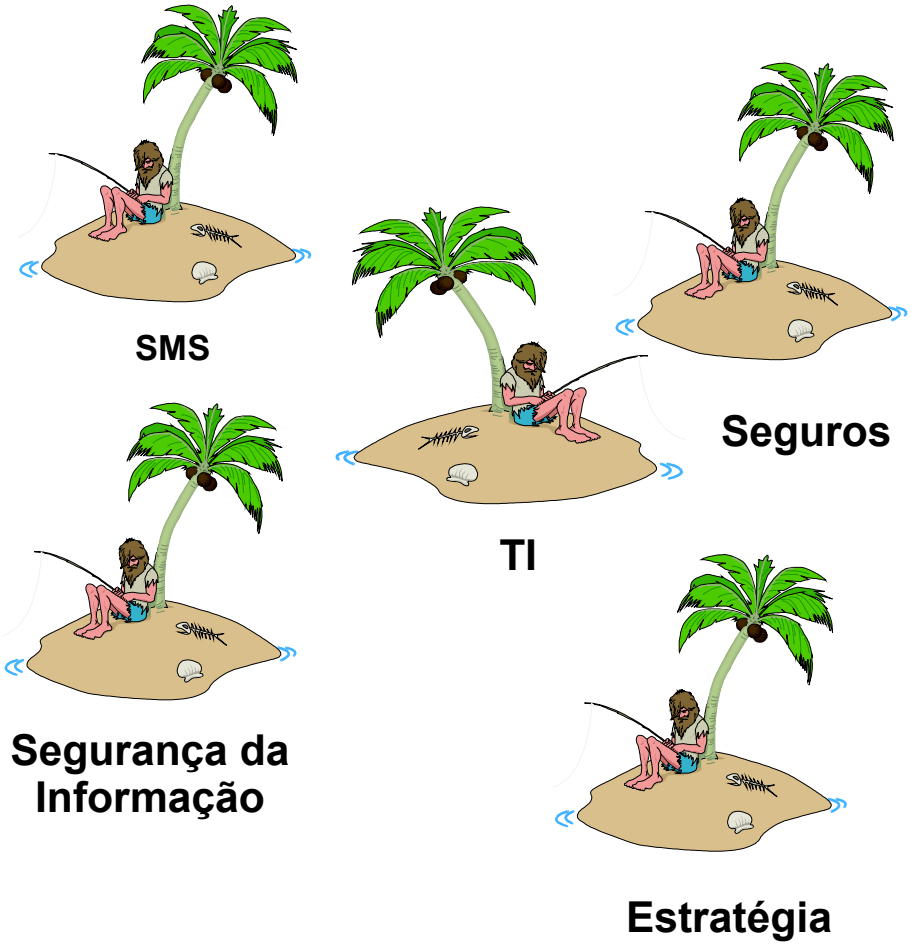
ISO 31000
Gestão de Riscos - Framework

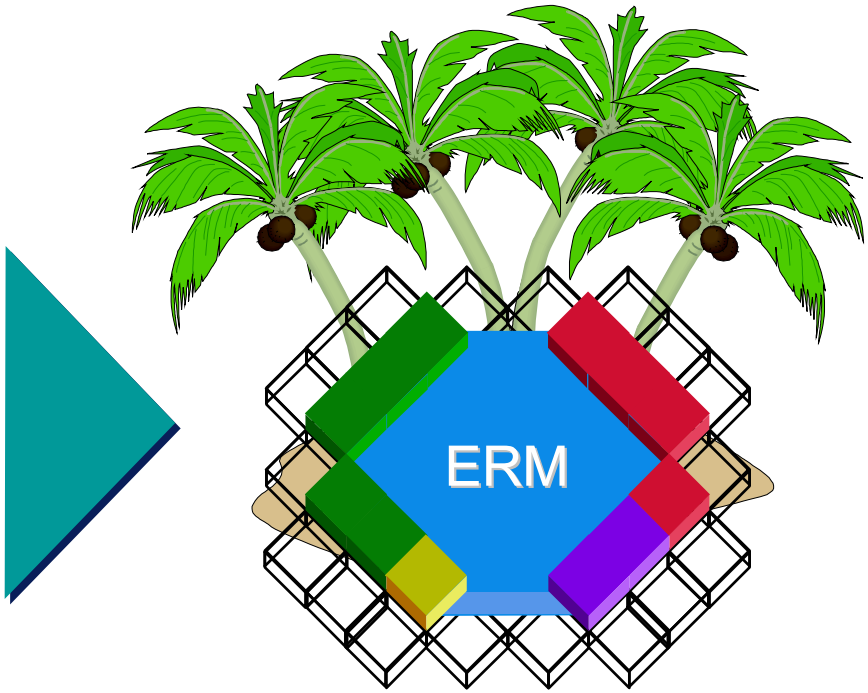


ISO 31000
Gestão de Riscos - Processo



Gestão de Riscos Empresariais



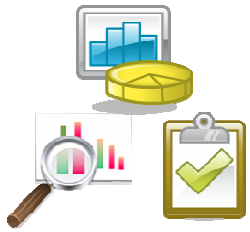


Modelos isolados

Integração

MODULO
Solutions for GRC

Gestão por Indicadores

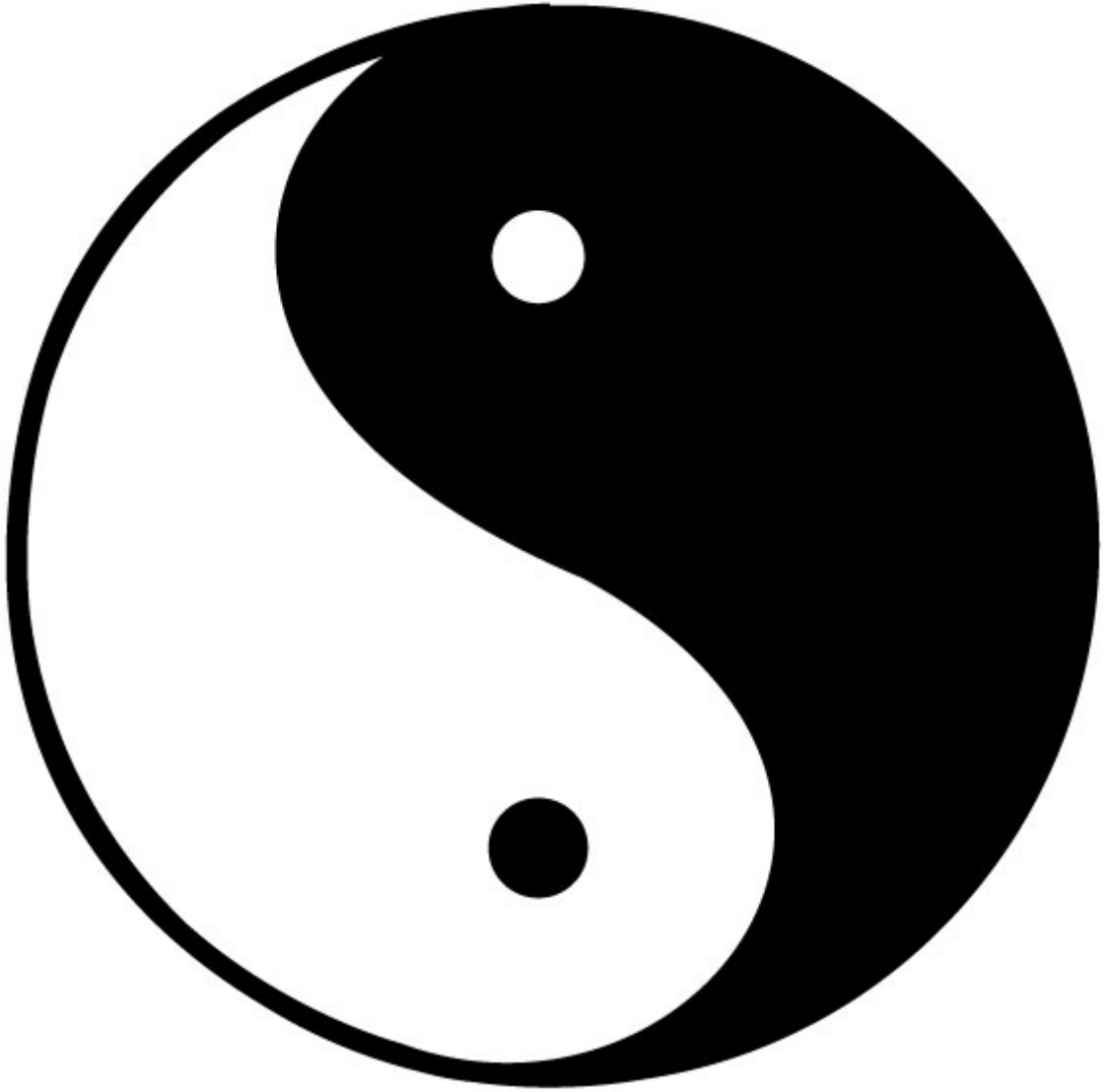


ISO 27001
ISO 9001

IBM Security Forum
Soluções para um ambiente seguro

Chief Risk Office

GCN



ABNT NBR 15999
Gestão de Continuidade de Negócios

- NBR 15999-1:2007
  - Código de Prática
  - Norma BS 25999-1:2006

- NBR 15999-2:2008
  - Certificação

Primeiro Banco certificado BS 25999 no mundo!

Valor ONLINE

Ação da Nossa Caixa no SPB obtém certificado

De São Paulo
17/03/2008

O Banco Nossa Caixa foi certificado pela capacidade de gerenciar a continuidade de seus negócios no Sistema de Pagamentos Brasileiros (SPB) em caso de adversidades climáticas, desastres, atentados e terrorismo.

É o primeiro banco brasileiro a obter esse certificado, concedido pela British Standard Institution (BSI) que submeteu a instituição aos requisitos estabelecidos pela norma internacional BS 25999-2:2007 que examina a capacidade das empresas de gerenciar a continuidade de seus negócios

Segundo o diretor financeiro e de relações com investidores, Arno Meyer, a certificação "assegura a confiabilidade dos processos" clientes e investidores.

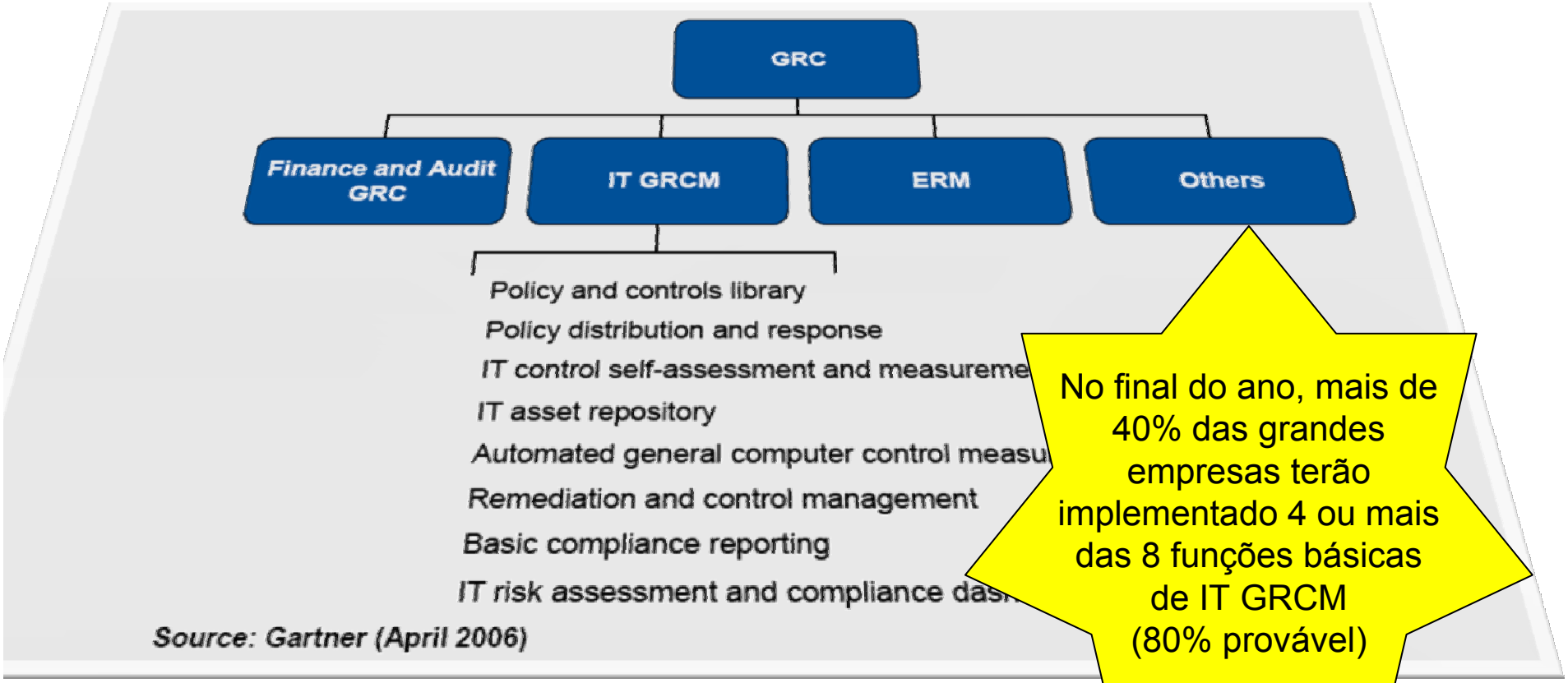
Gestão de Compliance

MÓDULO
Solutions for GRC

Governance + Risk + Compliance

IBM Security Forum
Soluções para um ambiente seguro

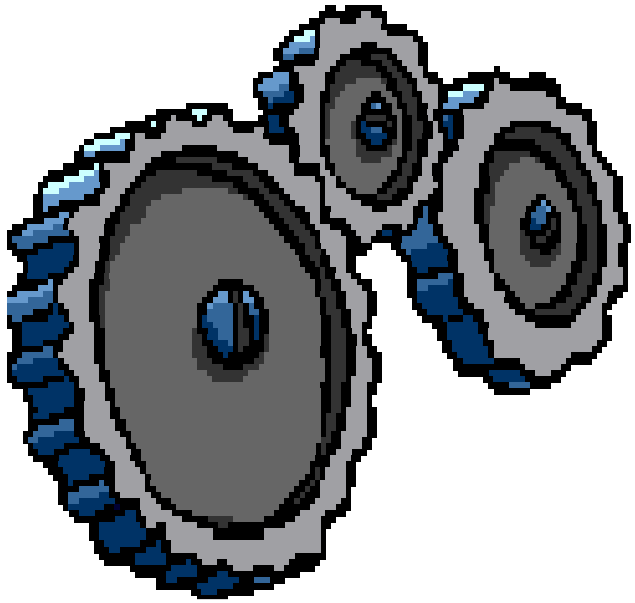
GRC Categorias



No final do ano, mais de 40% das grandes empresas terão implementado 4 ou mais das 8 funções básicas de IT GRCM (80% provável)

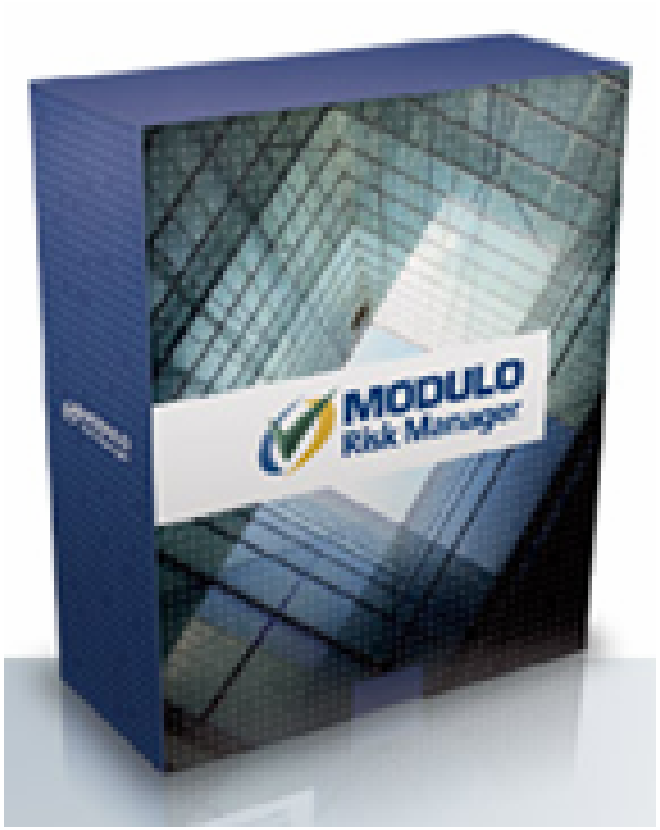
Automação da Gestão de Riscos

- umentar a produtividade da equipe
- rocesso estruturado e replicável
- oleta automática de informações
- nformações centralizadas
- elatórios, gráficos e consultas



Como podemos ajudar?

- Inventário heterogêneo
- ERM
- Bases de conhecimento
- Coleta heterogênea
- Análise
- Relatórios
- Painel de Controle (dashboard)
- Workflow (corretivo e preventivo)
- Plano de Contingência
- Gestão de Políticas



Para saber mais sobre GRC

Participe do sorteio de uma vaga!
Cartão de visita no estande da Módulo.

GRC Meeting 2009
Governança, Riscos e Compliance
Integração e Colaboração
7ª Edição

O Evento | Local | Programação | Palestrantes | Patrocinadores | Inscrições | Contatos | Dúvidas | Imprensa | Realizador | Edições Anteriores

GRC Meeting 2009: Integração e Colaboração.

Confira as vantagens de surfar esta nova onda

O Módulo Education convida para a 7ª edição do evento que reunirá os principais gestores do Brasil.

Diante do atual cenário financeiro mundial, devemos definir quais são as melhores práticas de Governança, Governança Corporativa e Governança de TI, bem como traçar as melhores estratégias para a gerência dos eminentes riscos e proteção das informações e dos negócios. Neste contexto, é fundamental a análise profunda dos novos parâmetros e a fomentação de novas bases para as consequentes mudanças políticas e de procedimentos corporativos.

Prepare-se para reconhecer grandes oportunidades em momentos de crise
Garanta já sua presença. Sua carreira agradece.

Zilta Marinho
Diretora de Educação
Módulo

Participe do sorteio de uma vaga!
Cartão de visita no estande da Módulo.

Patrocinadores:

MODULO Solutions for GRC

Apoiadores:

ABBI

ABGR

ABNT Associação Brasileira de Normas Técnicas

CNSeg

ISSA

ISO 27001

CERTIFICADA ISO 9001

IBM Security Forum
Soluções para um ambiente seguro

Obrigado!

Alberto Bastos, CISSP, MCSO

abastos@modulo.com.br

(21) 2123-4646

agenda

08h30 - 09h00	CREDENCIAMENTO E WELCOME COFFEE			
09h00 - 09h10	ABERTURA EXECUTIVA			
09h10 - 09h50	Segurança Integrada - Uma visão de Ponta a Ponta			
SESSÕES PARALELAS	Governança	Risco	PCI	Workshops - soluções de segurança
10h00-10h40	GRC - Governança, Riscos e Compliance	Ambientes Virtuais, Cybercrime, Novas tecnologias - As novas diretrizes da Segurança de Dados	Como manter-se em acordo com as 12 normas do PCI	Gerencie riscos de negócios associados as informações armazenadas
10h40 - 11h10	COFFEE BREAK - ÁREA DE PATROCINADORES			
11h10 - 11h50	Soluções de Alta Disponibilidade, Continuidade de Negócios e Resiliência	Gestão de riscos no contexto da norma internacional ISO-27005	Panorama de PCI-DSS no mercado brasileiro	Conformidade PCI e Segurança de aplicações Web
12h00 - 13h30	ALMOÇO			
13h40 - 14h20	Federação de Identidades: Conceitos e Cases	Conheça o Sistema de Verificação de Identidade com Biometria Facial	Conformidade com PCI-DSS - Lições Práticas	Garantindo flexibilidade, segurança e governança em ambientes SOA com WebSphere DataPower e WSRR
14h30 - 15h10	Problemas Comuns de Implementações em Gestão de Identidade	Reduzindo custos operacionais de segurança, de forma garantida e eficaz	Atendendo os requerimentos do PCI com Autenticação Forte	Segurança de informação com Gerenciamento de identidades e acessos - Uma poderosa combinação
15h10- 15h40	COFFEE BREAK - ÁREA DE PATROCINADORES			
15h40 - 16h20	Um framework para gestão pró-ativa de segurança	Proteção de Alto desempenho para Backbones	Sessão Patrocinador	Soluções Preventivas de Segurança. Proteja sua rede e dados, reduzindo custos operacionais associados a perdas e paradas
16h30 - 17h10	Plenária de Encerramento - Painel PCI			