Deloitte.

Take the right steps
9 principles for building the Risk Intelligent Enterprise™

Instituto Superior de Contabilidade e Administração de Coimbra
Junho 2009

The Risk Intelligent Enterprise™

The Risk Intelligent Enterprise™

"Risco: a probabilidade de perda ou a menor oportunidade de ganho causada por factores que afectam inadvertidamente o cumprimento dos objectivos da organização."

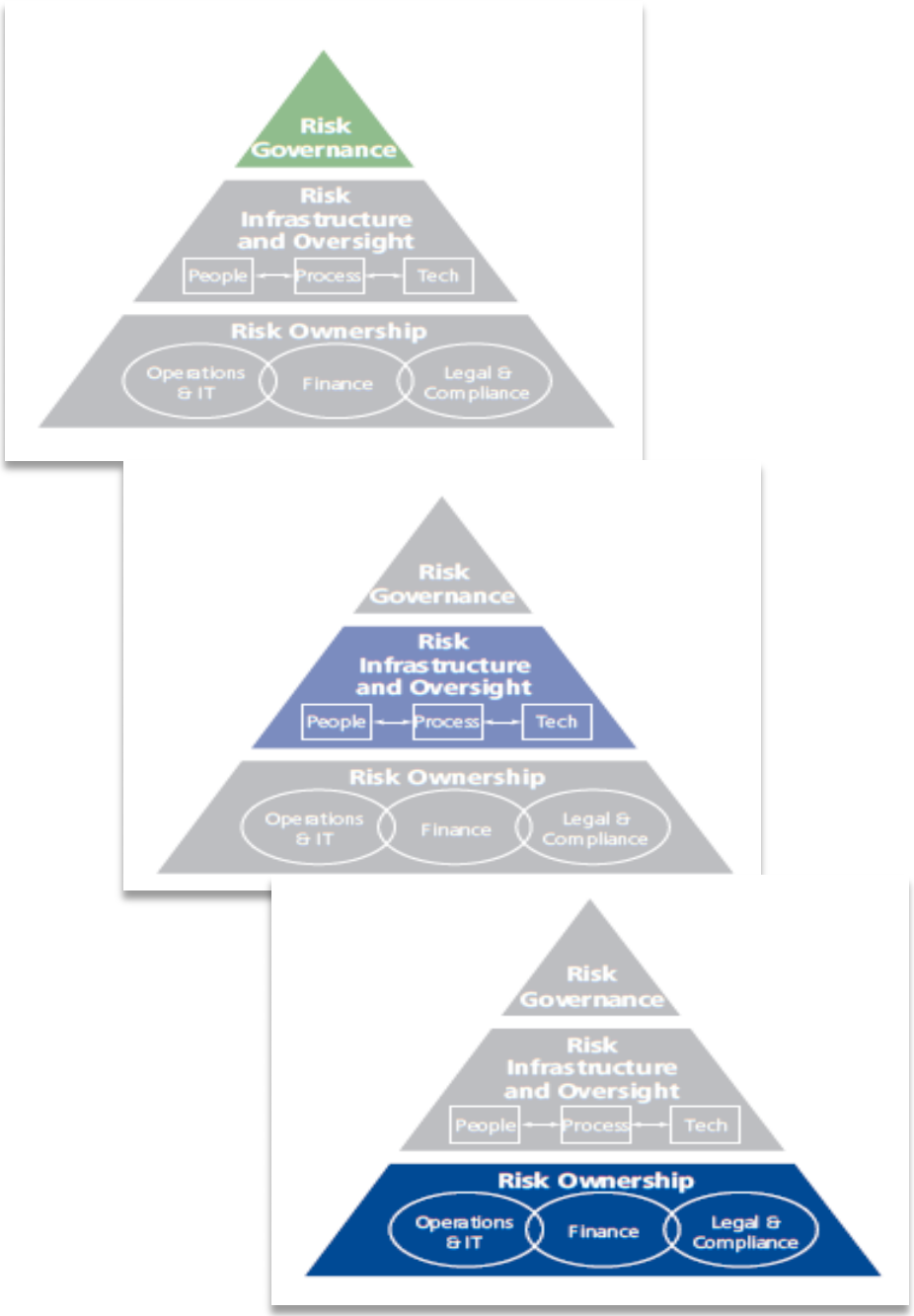
Poderão duas pessoas olhar para o mesmo objecto e ver duas realidades totalmente diferentes?

Todos têm uma visão do mundo condicionada pelo seu conhecimento ou experiência.

O Risco não pode mais ser visto a um nível de intuição, com abordagens de gestão *ad hoc* e reactivas.

Uma Risk Intelligent Enterprise™ é o local onde todos utilizam o mesmo par de óculos de Risco, partilham uma visão comum sobre Risco e adoptam uma *framework* comum para alinhamento das actividades relacionadas com Risco.

The Risk Intelligent Enterprise™



O objectivo principal numa Risk Intelligent Enterprise™ não é eliminar o contributo que cada indivíduo tem na Gestão dos Riscos da Organização, mas sobretudo fomentar a comunicação entre todos os intervenientes na Gestão de Risco através numa cultura corporativa de Risk Intelligence:

- *Risk Governance*
- *Risk Infrastructure and Oversight*
- *Risk Ownership*

Evoluir para um patamar de Risk Intelligent Enterprise™ consiste sobretudo em adoptar um conjunto de 9 princípios estruturantes e orientados para os principais níveis de gestão da Organização.

Princípio #1: Será um Risco uma ameaça ou uma oportunidade?

Será um Risco uma ameaça ou uma oportunidade?

Princípio #1: Será um Risco uma ameaça ou uma oportunidade?

Uma Risk Intelligent Enterprise™ tem uma definição de Risco comum que considera a preservação e a criação de valor, e aplica-a de forma consistente por toda a Organização.

Risco é um tópico de discussão muitas vezes evitado nas organizações sobretudo por ser associado por muitos a ameaças ou perdas.

No entanto, o tema Risco é cada vez mais encarado pelo seu factor gerador de oportunidade e valor na organização, ou seja, aceitar Risco como forma de recompensa.

Introdução de novos produtos no mercado, investimento em novos mercados ou avançar em estratégias de aquisição são hoje iniciativas desafiantes nas organizações em que uma abordagem de Risco é um factor crítico de sucesso.

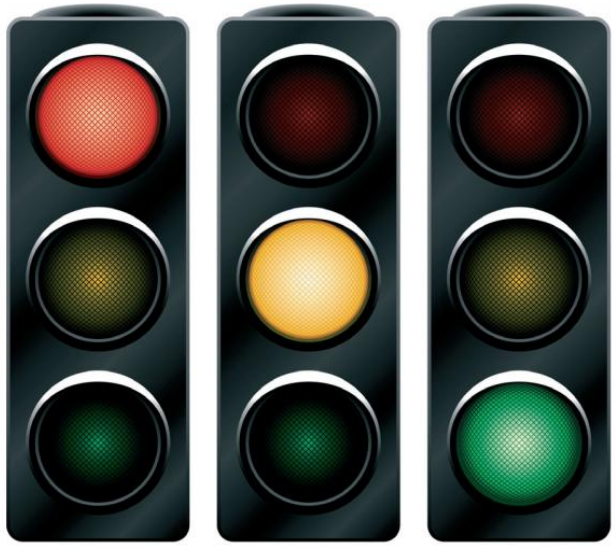
É portanto importante adoptar na organização uma definição lata de Risco, uma abordagem que considere uma gestão de risco orientada ao crescimento e à rentabilidade.

Princípio #2: Um modelo de Gestão de Risco alinhado com as necessidades

Um modelo de Gestão de Risco alinhado com as necessidades

Princípio #2: Um modelo de Gestão de Risco alinhado com as necessidades

Uma Risk Intelligent Enterprise™ utiliza um modelo de gestão de Risco comum alinhado com as boas práticas e com as principais expectativas das áreas da Organização.



A gestão de Risco é em muitas organizações descentralizada conduzindo a abordagens fragmentadas, duplicação de esforços e fontes de informação de Risco dispersas.

Para que um programa de gestão de risco corporativo resulte é necessário que o mesmo se enquadre numa framework comum (e.g. COSO ERM ou ISO 31000).

Uma visão integrada da gestão de risco capacita a organização na tomada de decisão de quais as oportunidades a perseguir e quais as ameaças a evitar.

É por isto que a framework deverá ser robusta para que possa suportar os objectivos corporativos de gestão de risco, possibilitando uma visão única da estratégia, iniciativas e estrutura de gestão, assegurando a conformidade legal e normativo do contexto da organização.

Não importa discutir qual a melhor framework a usar, desde que se garanta que a solução adoptada está alinhada com as necessidades da organização

Princípio #3: Uma Gestão de Risco coordenada e comunicada

Uma Gestão de Risco coordenada e comunicada

Princípio #3: Uma Gestão de Risco coordenada e comunicada

Uma Risk Intelligent Enterprise™ define claramente e formalmente a função, responsabilidade e autoridade pela Gestão de Risco na Organização.

Uma boa gestão de Risco é um esforço coordenado, onde as várias funções da organização são envolvidas de forma integrada.

Muitos são os que na organização se demitem da responsabilidade da gestão de Risco por assumirem que a gestão de Risco é uma competência de outros. Alterar esta mentalidade é um factor crítico de sucesso.

Promover o Risk Intelligence numa organização é comunicar de forma clara a todos os níveis da organização o que significa Risk Intelligence, porque é importante e quais as obrigações individuais no alcançar do sucesso da iniciativa.

Para tal é necessário assegurar bons canais de comunicação, cultura de Risco, programas de recompensa com base em Risco e programas de formação e treino adequados.

A gestão de Risco resulta quando o *board* define a direcção, a gestão orienta o programa, as áreas implementam e as funções críticas suportam a iniciativa (RH, TI, Auditoria, etc).

Princípio #4: Uma linguagem comum

Uma linguagem comum

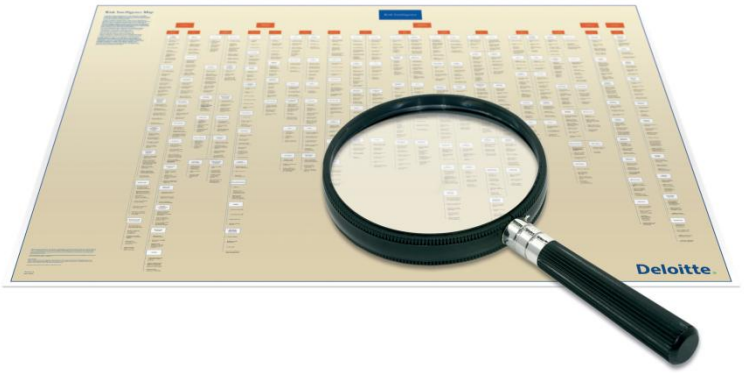
Princípio #4: Uma linguagem comum

Uma Risk Intelligent Enterprise™ tem definido um modelo de suporte às áreas operacionais no cumprimento das suas responsabilidades de Gestão de Risco.

Os especialistas de Risco tendem a comportar-se como qualquer grupo social: Mantém-se unidos e tendem a a fechar-se nos seus interesses. O Risco não pode ser visto de forma isolada pelo que a sua gestão também não poderá.

Acabar com silos de competências é um factor crítico de sucesso na gestão eficaz e eficiente do Risco. Criar pontes entre as unidades funcionais na organização assegurará linguagens comuns, adopção de processos e tecnologias consistentes e racionalização de recursos.

A utilização de ferramentas tais como o The Risk Intelligence Map™ são factores facilitadores que podem colocar a organização a pensar e falar na mesma linguagem, utilizando abordagens *standard*.

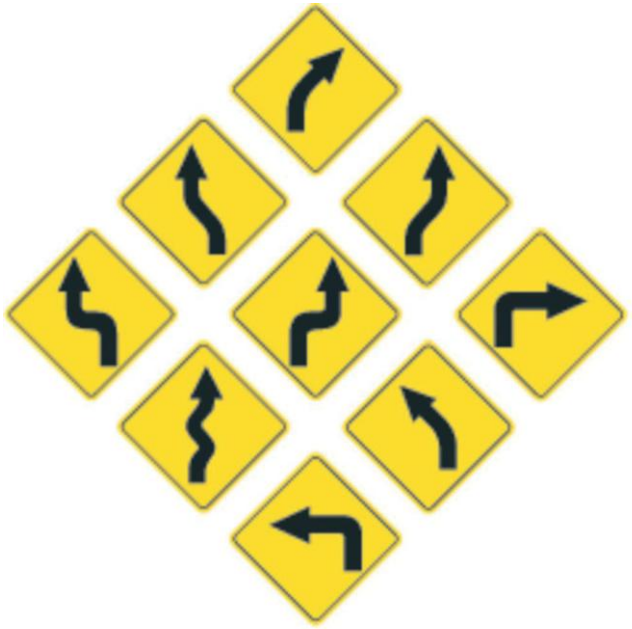


Princípio #5: Riscos conhecidos

Riscos conhecidos

Princípio #5: Riscos conhecidos

Uma Risk Intelligent Enterprise™ tem definidos canais que asseguram aos órgãos de governo e gestão (Administração, Comité de auditoria, etc.) a visibilidade sobre as práticas de Gestão de Risco e capacitem a sua tomada de decisão.



A informação de Risco e a forma como estes são geridos nem sempre circula nos diferentes níveis da organização. É da responsabilidade do board assegurar que a gestão tem à sua disposição o conhecimento de Risco necessário à tomada de decisão. Para tal, é necessário assegurar que :

- O tema Risco está na agenda da organização. Pensar e discutir o Risco antes que sejam forçados a analisar certezas;
- A estrutura de riscos é avaliada. Como estão os Riscos a ser geridos? Como são tratados os Riscos transversais?
- Os riscos são revistos periodicamente pela Gestão, nomeadamente os Riscos de implementação das Estratégias críticas.
- Os cenários de Risco são discutidos. Onde estão as melhores oportunidades? O que poderá impedir a organização de alcançar os seus objectivos estratégicos?
- Avaliar a apetência ao Risco. Determinar os níveis de aceitação de Riscos residuais
- Assegurar avaliação independente. Assegurar uma revisão interna/externa da efectividade do programa de gestão de Risco.

Princípio #6: Abordagem *Top-Down* do Risco

Abordagem *Top-Down* do Risco

Princípio #6: Abordagem *Top-Down* do Risco

Uma Risk Intelligent Enterprise™ atribui a responsabilidade à gestão de topo pelo desenho, implementação e manutenção de um programa efectivo de Gestão de Risco.

A responsabilidade pelo Risco é de todos, sendo maior aos níveis Executivos e de Gestão onde a liderança e autoridade deverá influenciar o pensamento de Risco a todos os níveis na organização.

A Gestão de Topo é responsável por garantir que o risco seja reconhecido como factor de recompensa, assegurar a gestão de Risco a todos os níveis da organização, gerir expectativas, assegurar responsabilidade e compromisso, potenciar a mudança e melhoria contínua, implementar uma cultura de Risk Intelligence na organização.

Será esta uma agenda ambiciosa? Como será possível assegurar todos estes compromissos? Um dos factores críticos de sucesso é a constituição de um Risk Intelligence group — um comité a um nível executivo — que assegure a gestão do programa na organização.

Algumas organizações estão já a definir os seus Chief Risk Officer (CRO), elementos importantes na articulação do tema Risk Intelligence com os principais órgãoes de gestão e decisão ao nível da gestão de topo.

Princípio #7: Responsabilidade pelo Risco

Responsabilidade pelo Risco

Princípio #7: Responsabilidade pelo Risco

Uma Risk Intelligent Enterprise™ atribui às áreas de negócio a responsabilidade pelo seu desempenho mas também pela Gestão dos Riscos que assumem no modelo de Gestão de Risco definido pela gestão de topo.

.

A responsabilidade pelo Risco é de todos, mas quem é o seu "dono"?

O *ownership* do Risco é um tema complexo nas organizações, portanto simplifiquemos: Se é *owner* da unidade de negócio então é *owner* dos seus Riscos. Por outras palavras, se é responsável pelo sucesso de uma unidade de negócio então é igualmente responsável pela gestão contínua dos riscos associados com essa unidade, ainda que a mesma possa ser partilhada com os demais colaboradores.

O que envolve ser responsável pelo Risco? Entre outras responsabilidades, os Risk owners são responsáveis pela identificação, avaliação, monitorização, controlo e reporte para a Gestão Executiva, promoção da consciencialização para o Risco e gestão das actividades de resposta aosRiscos.

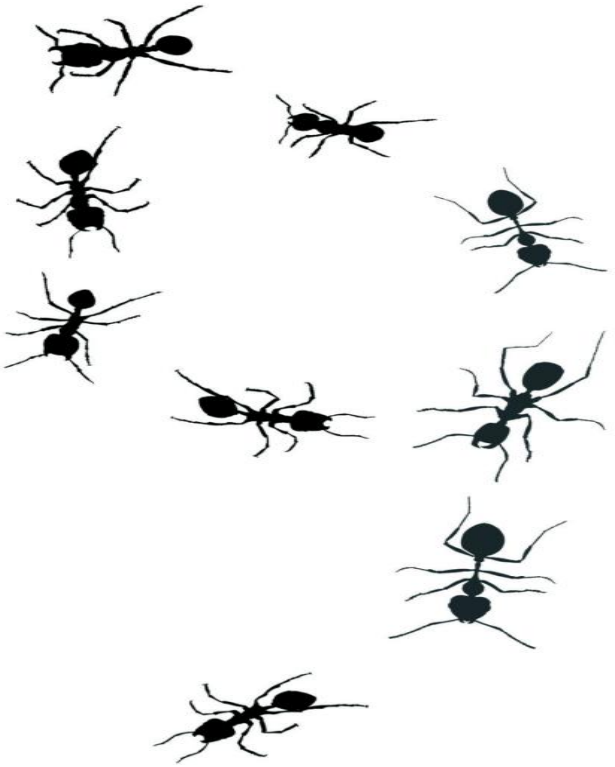
No entanto, a actividade do owner do Risco deverá ser sempre condicionada pelas *frameworks* corporativas e enquadrada nas políticas, normas e procedimentos definidas (e.g. nível de apetência/aceitação do Risco).

Princípio #8: Funções de suporte

Funções de suporte

Princípio #8: Funções de suporte

Uma Risk Intelligent Enterprise™ reconhece a importância de determinadas Funções (e.g., financeira, legal, IT, RH, etc.) no suporte às áreas de negócio e atribui-lhes responsabilidades directas no programa de Gestão de Risco.



Algumas Funções, incluindo a Financeira, Legal, Recursos Humanos, Tax e TI, diferem das áreas de negócio pelo facto de não apenas serem *owners* de Risco – são Funções que suportam Riscos.

Tal como as áreas de negócio, estas Funções são primariamente responsáveis pelos Riscos originados nas suas operações, mas as suas responsabilidade extravasam este tipo de Riscos.

Como exemplo, para além da responsabilidade primária pelos Riscos tecnológicos, a área de TI deverá ser uma área de suporte importante na monitorização e mitigação de riscos de negócio.

A transversalidade destas Funções na organização faz com que seja veículos importantes no desenvolvimento e implementação as políticas, procedimentos e controlos de mitigação de Riscos.

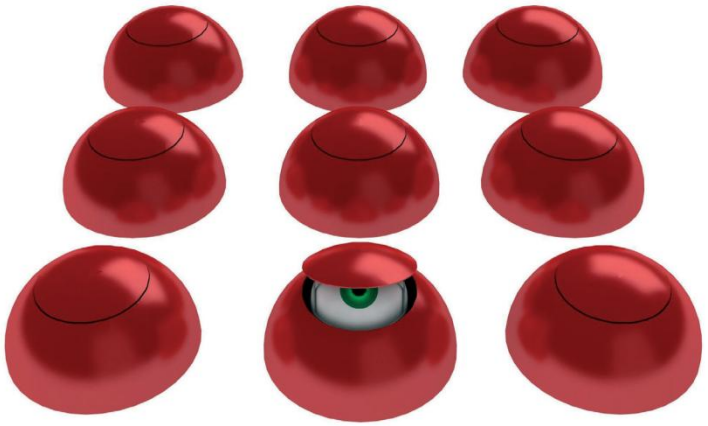
Importa que estas Funções chave sejam envolvidas nos comités, foruns e equipas de Risco com papéis formalmente definidos e alinhados com a *framework* de Risco corporativa.

Princípio #9: Os observadores

Os observadores

Princípio #9: Os observadores

Uma Risk Intelligent Enterprise™ atribui responsabilidades a determinadas funções (e.g. Auditoria Interna, Gestão de Risco, Conformidade) pela revisão, monitorização do programa de Gestão de Risco e reporte aos órgãos de governo e gestão da Organização.



Funções como a Auditoria Interna, Controlo Interno, Risco e Compliaance desempenham papéis chave na Gestão de Risco da Organização, nomeadamente ao assegurarem a operacionalidade efectiva das estruturas de Risco e Controlo.

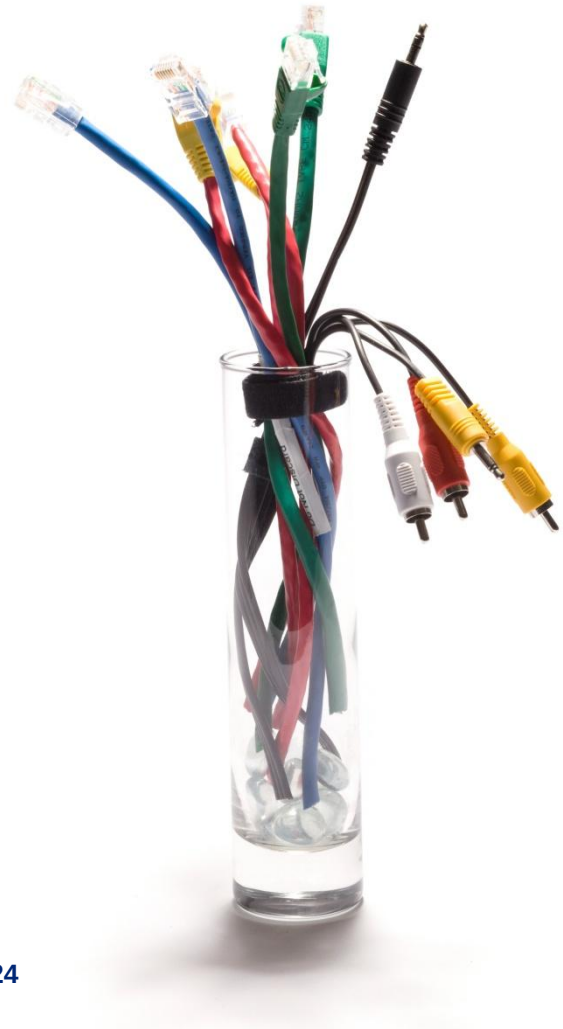
Eestas Funções desempenham papéis importantes designadamente:

- Avaliação do estado actual da Gestão de Risco, apoiando a Gestão na identificação de futuros Riscos e Oportunidades.
- Avaliar se a organização aceita Riscos a um nível que é capaz de gerir.
- Validar que a organização assegura uma Gestão de Risco integrada e gerida a um nível adequado.
- Identificar e eliminar ineficiências na Gestão de Risco.
- Identificar áreas com insuficiênte cobertura de Risco e assegurar recursos para regularização.
- Providenciar conhecimento adicional em áreas específicas de Risco (e.g. Fraude).
- Suportar a avaliação, correcção e redesenho de Riscos e Controlos

The Risk Intelligent IT Internal Auditor

The Risk Intelligent IT Internal Auditor

"Aqui está a verdade de muitas organizações: A Auditoria Interna TI auditou UNIX durante os últimos 5 anos. A Auditoria Interna TI auditará novamente UNIX este ano. Nada muda!"



Para manter (ou ganhar) a sua importância, a Auditoria Interna TI terá de evoluir. Acutalmente, Auditoria TI não é mais uma auditoria de Sistemas (nunca foi realmente mas isso é outro tema). Auditoria TI é hoje ter um entendimento global do negócio da organização, entendendo o valor que a tecnologia representa nos objectivos da organização. Auditoria TI é também adoptar abordagens de Risk Intelligent que não apenas se foquem em perdas mas que que também potenciem a identificação de oportunidades.

Qual o tipo de Auditoria TI na sua organizção?

Tipo 1 – *A pairar*: A Auditoria TI cumpre com o seu plano anual, realiza auditoria típicas de CGI e Sistemas, cumprindo com as suas tarefas mas sem objectivos claramente definidos na organização.

Tipo 2 – *A descolar*: A Auditoria TI inicia a sua participação na organização. O grupo apoia e intervém em projectos correntes tais como M&A, implementações de sistemas e avaliações de Risco.

Tipo 3 – *A voar alto*: A Auditoria TI apresenta uma visão clara do futuro da organização. O grupo é envolvido na criação de valor, contribuindo para a aplicação dos princípios de Risk Intelligence, identificando Riscos antes que estes se transformem em factos.

Missão impossível?

Contactos

Deloitte.

Bruno Horta Soares
Manager

Deloitte & Associados, SROC, S.A.
Edifício Atrium Saldanha
Praça Duque de Saldanha, 1 - 6º
1050-094 Lisboa
Portugal

Tel: +(351) 21 042 75 32
Fax: +(351) 21 042 79 50
bsoares@deloitte.pt
www.deloitte.com/pt

Member of
Deloitte Touche Tohmatsu